Symantec AntiVirus™ for SMTP Gateways Implementation Guide

symantec.™

Symantec AntiVirus™ for SMTP Gateways Implementation Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version 3.1 PN: 10052277

Copyright Notice

Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY. The technical documentation is being delivered to you AS-IS, and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice. No part of this publication may be copied without the express written permission of Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

Trademarks

Symantec, the Symantec logo, and Norton AntiVirus are U.S. registered trademarks of Symantec Corporation and its subsidiaries. Symantec AntiVirus, Symantec Web Security, LiveUpdate, Bloodhound, Symantec Antivirus Research Center (SARC), Symantec Security Response, and Symantec pcAnywhere are trademarks of Symantec Corporation and its subsidiaries. Sun, Sun Microsystems, the Sun logo, and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc., in the United States and other countries. Sendmail is a trademark of Sendmail, Inc. SPARC is a registered trademark of SPARC International, Inc. Products bearing SPARC trademarks are based on an architecture developed by Sun Microsystems, Inc. VeriSign is a registered trademark of VeriSign in the United States and other countries. Microsoft, Windows, Windows NT, Visual Basic, MS-DOS, JScript, Visio, and the Windows logo are registered trademarks or trademarks of Microsoft Corporation in the United States and other countries. Netscape Navigator is a registered trademark of Netscape Communications Corporation in the United States and other countries. Intel and Pentium are registered trademarks of Intel Corporation. Adobe, Acrobat, and Reader are registered trademarks of Adobe Systems Incorporated in the United States and other countries.

THIS PRODUCT IS NOT ENDORSED OR SPONSORED BY ADOBE SYSTEMS INCORPORATED, PUBLISHERS OF ADOBE ACROBAT.

Other brands and product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Printed in the United States of America.
10 9 8 7 6 5 4 3 2 1

Technical support

As part of Symantec Security Response, the Symantec global Technical Support group maintains support centers throughout the world. The Technical Support group's primary role is to respond to specific questions on product feature/ function, installation, and configuration, as well as to author content for our Web-accessible Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering as well as Symantec Security Response to provide Alerting Services and Virus Definition Updates for virus outbreaks and security alerts.

Symantec technical support offerings include:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web support components that provide rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Content Updates for virus definitions and security signatures that ensure the highest level of protection
- Global support from Symantec Security Response experts, which is available 24 hours a day, 7 days a week worldwide in a variety of languages
- Advanced features, such as the Symantec Alerting Service and Technical Account Manager role, offer enhanced response and proactive security support

Please visit our Web site for current information on Support Programs. The specific features available may vary based on the level of support purchased and the specific product that you are using.

Licensing and registration

If the product that you are implementing requires registration and/or a license key, the fastest and easiest way to register your service is to access the Symantec licensing and registration site at www.symantec.com/certificate. Alternatively, you may go to www.symantec.com/techsupp/ent/enterprise.html, select the product that you wish to register, and from the Product Home Page, select the Licensing and Registration link.

Contacting Technical Support

Customers with a current support agreement may contact the Technical Support group via phone or online at www.symantec.com/techsupp

Customers with Platinum support agreements may contact Platinum Technical Support via the Platinum Web site at www-secure.symantec.com/platinum/

When contacting the Technical Support group, please have the following:

- Product release level
- Hardware information
- Available memory, disk space, NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description
  - Error messages/log files
  - Troubleshooting performed prior to contacting Symantec
  - Recent software configuration changes and/or network changes

Customer Service

To contact Enterprise Customer Service online, go to www.symantec.com, select the appropriate Global Site for your country, then choose Service and Support. Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advice on Symantec's technical support options
- Nontechnical presales questions
- Missing or defective CD-ROMs or manuals

SYMANTEC SOFTWARE LICENSE AGREEMENT
ENTERPRISE ANTIVIRUS SOFTWARE

THIS LICENSE AGREEMENT SUPERSEDES THE LICENSE AGREEMENT CONTAINED IN THE SOFTWARE INSTALLATION AND DOCUMENTATION.

SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES (“SYMANTEC”) IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS “YOU OR YOUR”) ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND THE LICENSOR. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING ON THE “AGREE” OR “YES” BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK ON THE “I DO NOT AGREE” OR “NO” BUTTON, OR OTHERWISE INDICATE REFUSAL AND MAKE NO FURTHER USE OF THE SOFTWARE.

1. LICENSE:

The software and documentation that accompanies this license (collectively the “Software”) is the proprietary property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, You will have certain rights to use the quantity of the Software for which You have paid the applicable license fees after Your acceptance of this license. This license governs any releases, revisions, or enhancements to the Software that the Licensor may furnish to You. Except as may be modified by an applicable Symantec license certificate, license coupon, or license key (each a “License Module”) that accompanies, precedes, or follows this license, Your rights and obligations with respect to the use of licensed copies of this Software are as follows:

YOU MAY:

A. use the Software in the manner described in the Software documentation and in accordance with the License Module. If the Software is part of an offering containing multiple Software titles, the aggregate number of copies You may use may not exceed the aggregate number of licenses indicated in the License Module, as calculated by any combination of licensed Software titles in such offering. Your License Module shall constitute proof of Your right to make such copies. If no License Module accompanies, precedes, or follows this license, You may make one copy of the Software You are authorized to use on a single machine;

B. make one copy of the Software for archival purposes, or copy the Software onto the hard disk of Your computer and retain the original for archival purposes;

C. use the Software on a network or to protect a network such as at the gateway or on a mail server, provided that You have a license to the Software for each computer that can access the network;

D. after written consent from Symantec, transfer the Software on a permanent basis to another person or entity, provided that You retain no copies of the Software and the transferee agrees to the terms of this license; and

E. use the Software in accordance with any additional permitted uses set forth in Section 8 below.

YOU MAY NOT:

A. copy the printed documentation which accompanies the Software;

B. sublicense, rent or lease any portion of the Software; reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;

C. use a previous version or copy of the Software after You have received a disk replacement set or an upgraded version. Upon upgrading the Software, all copies of the prior version must be destroyed;

D. use a later version of the Software than is provided herewith unless You have purchased corresponding maintenance and/or upgrade insurance or have otherwise separately acquired the right to use such later version;

E. use, if You received the software distributed on media containing multiple Symantec products, any Symantec software on the media for which You have not received a permission in a License Module;

F. use the Software in any manner not authorized by this license; nor

G. use the Software in any manner that contradicts any additional restrictions set forth in Section 8 below.

2. CONTENT UPDATES:

Certain Symantec software products utilize content that is updated from time to time (antivirus products utilize updated virus definitions; content filtering products utilize updated URL lists; some firewall products utilize updated firewall rules; vulnerability assessment products utilize updated vulnerability data, etc.; collectively, these are referred to as “Content Updates”). You may obtain Content Updates for any period for which You have purchased upgrade insurance for the product, entered into a maintenance agreement that includes Content Updates, or otherwise separately acquired the right to obtain Content Updates. This license does not otherwise permit You to obtain and use Content Updates.

3. LIMITED WARRANTY:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to You. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money You paid for the Software. Symantec does not warrant that the Software will meet Your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

4. DISCLAIMER OF DAMAGES:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT

OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO CASE SHALL SYMANTEC'S LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether You accept the Software.

5. U.S. GOVERNMENT RESTRICTED RIGHTS:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are "Commercial Items", as that term is defined in 48 C.F.R. section 2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation", as such terms are defined in 48 C.F.R. section 252.227-7014(a)(5) and 48 C.F.R. section 252.227-7014(a)(1), and used in 48 C.F.R. section 12.212 and 48 C.F.R. section 227.7202, as applicable. Consistent with 48 C.F.R. section 12.212, 48 C.F.R. section 252.227-7015, 48 C.F.R. section 227.7202 through 227.7202-4, 48 C.F.R. section 52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec's computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014, United States of America.

6. EXPORT REGULATION:

Export or re-export of this Software is governed by the laws and regulations of the United States and import laws and regulations of certain other countries   Export or re-export of Software to any entity on the Denied Parties List and other lists promulgated by various agencies of the United States Federal Government is strictly prohibited.

7. GENERAL:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the laws of England. This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Software and: (i) supersedes all prior or contemporaneous oral or written communications, proposals and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment or similar communications between the parties. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software. The disclaimers of warranties and damages and limitations on liability shall survive termination. The original of this Agreement has been written in English and English is the governing language of this Agreement. This Agreement may only be modified by a License Module which accompanies this license or by a written document which has been signed by both You and Symantec. Should You have any questions concerning this Agreement, or if You desire to contact Symantec for any reason, please write to: (i) Symantec Customer Service, 555 International Way, Springfield, OR 97477, U.S.A. or (ii) Symantec Customer Service Center, PO BOX 5689, Dublin 15, Ireland.

8. ADDITIONAL RESTRICTIONS FOR SPECIFIED SOFTWARE:

A. If the Software You have licensed is a specified Symantec AntiVirus™ for a third-party product or platform, You may only use that specified Software with the corresponding product or platform. You may not allow any computer to access the Software other than a computer using the specified product or platform. In the event that You wish to use the Software with a certain product or platform for which there is no specified Software, You may use the Symantec AntiVirus Scan Engine.

B. If the Software you have licensed is Symantec AntiVirus for NetApp® Filer, the following additional use(s) and restriction(s) apply:

i) You may use the Software only with a NetApp Filer server;

ii) You may use the Software only with files accessed through a NetApp Filer; and

iii) You may not use the Software on a server that exceeds the specified capacity set forth in Your License Module.

C. If the Software you have licensed is Symantec AntiVirus for Web Servers, the following additional use(s) and restriction(s) apply:

i) You may use the Software only with files that are received from third parties through a Web server;

ii) You may use the Software only with files received from less than 10,000 unique third parties per month; and

iii) You may not charge or assess a fee for use of the Software for Your internal business.

D. If the Software You have licensed is Symantec Web Security, independent of version or operating platform designation, upon the expiration of Your right to acquire Content Updates, the filtering definitions corresponding with all previous Content Updates will be entirely deleted and will no longer be available for use with the Software. Upon the expiration of Your right to acquire Content Updates, access to updated virus definitions will no longer be available. However, You may continue to use virus definitions previously acquired.

E. If the Software You have licensed is Symantec AntiVirus Corporate Edition, You may not use the Software on or with devices on Your network running embedded operating systems specifically supporting network-attached storage functionality without separately licensing a version of such Software specifically licensed for a specific type of network-attached storage device under a License Module.

F. If the Software You have licensed is Symantec AntiVirus for EMC® Celerra™ File Server, You may use the Software only with EMC Celerra servers and only if You have a license to the Software for each Celerra AntiVirus Agent (CAVA) associated with each such server. You may not allow any computer to access the Software other than an EMC Celerra server.

NetApp is a registered trademark of Network Appliance, Inc., in the U.S. and other countries.

EMC and Celerra are trademarks or registered trademarks of EMC Corporation in the U.S. and other countries.

Contents

Chapter 3 Configuring Symantec AntiVirus for SMTP Gateways

Chapter 4 Setting your blocking policy

Chapter 5 Setting your antivirus policy

Chapter 6 Notifications, logging, and reporting

Chapter 7 Integrating Symantec AntiVirus for SMTP Gateways with SESA

Index

CD Replacement Form

Introducing Symantec AntiVirus for SMTP Gateways

This chapter includes the following topics:

About Symantec AntiVirus for SMTP Gateways

Symantec AntiVirus for SMTP Gateways is a Simple Mail Transfer Protocol (SMTP) server that processes email before sending it to a local mail server for delivery. It can be configured to protect your network in four ways:

- Block unwanted email messages.
- Scan and repair infected email attachments (files appended to email messages) and infected files within attachments.
- Block spam.
- Prevent the relaying of spam for another host.

The email gateway is only one way that a virus can penetrate your network. For comprehensive virus protection, install both Symantec AntiVirus for SMTP Gateways and appropriate workstation or server versions of antivirus protection on every computer at your site.

For a complete listing of Symantec antivirus products, visit www.symantec.com.

What’s new in Symantec AntiVirus for SMTP Gateways

Symantec AntiVirus for SMTP Gateways maintains all of the functionality of past Symantec antivirus products, and includes the new features of Symantec AntiVirus for SMTP Gateways, versions 3.0 and 3.1, in Table 1-1.

Table 1-1 New features of Symantec AntiVirus for SMTP Gateways

Description	New feature
Improved usability and easier configuration	■ Redesigned administrative interface

Table 1-1 New features of Symantec AntiVirus for SMTP Gateways

Description	New feature
Improved management options	■ Symantec Enterprise Security Architecture (SESA) integration ■ Notifications for content violations ■ Customizable sender email address ■ System alerts for administrators ■ Message forwarding for content violations ■ Process pausing during virus threats ■ Hold queue for unscannable messages ■ Enhanced status screen and reporting ■ Report-only administrator option
Enhanced security	■ Secure Sockets Layer (SSL) encryption for logon- and password-changing sessions ■ Prevention of denial-of-service (DoS) attacks ■ Scanning of malformed Multipurpose Internet Mail Extensions (MIME) messages ■ Alerting for virus outbreaks
Enhanced antispam controls	■ Blocking by domain and email address ■ Blocking by Domain Name System black lists (DNSBL) ■ Wildcard support in routing list
Enhanced blocking	■ Prevention of spam relaying by blocking special characters in senders' addresses
Enhanced processing	■ In-container rename and replace ■ Auto refresh of configuration file (no need to restart service for changes to take effect) ■ Slow queue reordering that moves messages that cannot be delivered to the rear of the queue and messages that can be delivered to the front
Enhanced diagnostic features	■ Queue file save capability ■ SMTP conversation logging

Components of Symantec AntiVirus for SMTP Gateways

Symantec AntiVirus for SMTP Gateways consists of several components that work together to protect your network.

Table 1-2 lists Symantec AntiVirus for SMTP Gateways components and their descriptions.

Table 1-2 Symantec AntiVirus for SMTP Gateways components

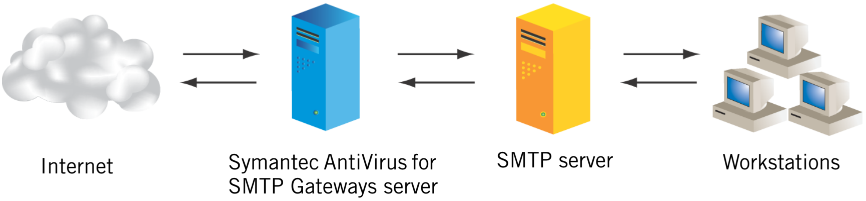
Component	Description
Symantec AntiVirus for SMTP Gateways	This is the software that you install to protect network servers and workstations. It protects computers from viruses in email attachments, blocks unwanted content, and prevents spam and spam relaying.
LiveUpdate™ Administration Utility	LiveUpdate lets Symantec products download program and virus definitions files updates directly from Symantec or from an intranet LiveUpdate server. With the LiveUpdate Administration Utility, you can configure one or more intranet FTP, HTTP, or LAN servers to act as internal LiveUpdate servers. For more information, see the *LiveUpdate™ Administrator's Guide* on the CD.
Symantec Central Quarantine	You can configure Symantec AntiVirus for SMTP Gateways to automatically forward infected attachments from local quarantine servers to Symantec Central Quarantine, a central repository for infected attachments. You can configure Symantec Central Quarantine to automatically send files that it cannot repair to Symantec Security Response for analysis and repair. For more information, see the *Symantec™ Central Quarantine Administrator's Guide* available on the CD.
Adobe® Acrobat® Reader®	This is the software that makes it possible to read documentation in .pdf format.

How Symantec AntiVirus for SMTP Gateways works

In a typical configuration, Symantec AntiVirus for SMTP Gateways operates as an SMTP server that accepts incoming email from the Internet, processes the email based on the configuration of the product, and delivers the email to another SMTP server for further processing and delivery. It also receives outgoing email from your SMTP server and processes it based on the configuration of Symantec AntiVirus for SMTP Gateways.

Figure 1-1 shows how Symantec AntiVirus for SMTP Gateways is typically configured on a network.

Figure 1-1 Typical processing path: Symantec AntiVirus for SMTP Gateways



When Symantec AntiVirus for SMTP Gateways receives an email message with an attachment from an Internet or internal network source, it decodes and decompresses the message. It sends the message to the fast queue (a logical queue with a large number of dedicated threads) to be processed. Symantec AntiVirus for SMTP Gateways first looks for messages to block before scanning for viruses. You can configure Symantec AntiVirus for SMTP Gateways to send notification to senders and administrators when messages are blocked.

After blocking messages, Symantec AntiVirus for SMTP Gateways uses several antivirus technologies to scan remaining messages for viruses. It looks for known viruses by comparing segments of your files to the sample code inside of a virus definitions file. The virus definitions file contains nonmalicious bits of code, or virus definitions, for thousands of viruses. If Symantec AntiVirus for SMTP Gateways finds a match, the file is infected, and the email is handled (repaired, deleted, or logged and delivered) according to how you have configured the software. To protect yourself from new viruses, you can configure regular virus definitions file updates.

See “Updating virus definitions files” on page 91.

By default, when Symantec AntiVirus for SMTP Gateways detects a virus in an email attachment (that is not a container file), it attempts to repair the infected attachment. If Symantec AntiVirus for SMTP Gateways cannot repair the attachment, by default, it deletes the attachment. With container files, Symantec AntiVirus for SMTP Gateways attempts to repair the files within the container file. If the file type supports replacing embedded files (for example, MIME, UUE, BinHex), and the embedded file cannot be cleaned, the embedded file is deleted and renamed DELETED*n*.TXT where *n* is used to number each deleted embedded file within the container file.

You can configure Symantec AntiVirus for SMTP Gateways to forward infected attachments to a Central Quarantine Server, and configure the Central Quarantine Server to automatically submit virus samples to Symantec Security Response™ for analysis. If Symantec AntiVirus for SMTP Gateways is configured not to quarantine anything, attachments that cannot be repaired are scanned in a temporary location and, if infected, they are deleted.

After blocking and scanning messages, Symantec AntiVirus for SMTP Gateways delivers them. If the message cannot be delivered, it is forwarded to the slow queue so as not to backlog the fast queue. Once the message is in the slow queue, Symantec AntiVirus for SMTP Gateways continues to attempt delivery of the message. Symantec AntiVirus for SMTP Gateways now reorders messages in the slow queue, moving messages that will not deliver to the rear of the queue, and moving to the front of the queue messages destined to the same host on the next hop (if those hosts are accepting delivery). If it is not able to be delivered within the specified number of days, the forwarding server returns a reason (wrong domain, user name doesn't exist, for example), and the file is deleted from the slow queue.

What you can do with Symantec AntiVirus for SMTP Gateways

Symantec AntiVirus for SMTP Gateways handles email attachments (files appended to email messages) according to your blocking and antivirus policies. You set your policies through the Symantec AntiVirus for SMTP Gateways administrative interface, from either the physical server on which the software is installed or from any workstation on the network.

See "Setting your blocking policy" on page 67 and "Setting your antivirus policy" on page 85.

You can configure Symantec AntiVirus for SMTP Gateways so that users on the network become aware of its operation only if a virus or content violation is detected. You can also configure Symantec AntiVirus for SMTP Gateways to send alerts to administrators in the case of system events, and notifications to administrators and senders when there is virus activity.

See "Configuring alerts" on page 58.

You also use the administrative interface to set antispam and relay settings.

Block email messages

Your blocking policy is determined by how you configure Symantec AntiVirus for SMTP Gateways to block messages (what criteria to use to block messages and attachments, and how those blocked messages and attachments are to be handled).

See "Setting your blocking policy" on page 67.

Symantec AntiVirus for SMTP Gateways can be configured to block messages based on the following:

- Message size
- Subject line
- File name
- Container limits
- Encrypted container
- Sender address
- Domain Name Server black list (DNSBL) antispam lists
- Heuristic spam detection (in conjunction with subject blocking)
- Characters in email address

Respond to viruses

Your antivirus policy is determined by how you configure Symantec AntiVirus for SMTP Gateways to handle email (for example, what file types to scan, what files to quarantine, and when to notify administrators and senders if viruses are found or virus outbreaks occur).

See "Setting your antivirus policy" on page 85.

Table 1-3 shows options for handling infected attachments.

Table 1-3 Options for handling infected attachments

Option	Description
Repair	The virus within the attachment is repaired, if possible.
Delete	No repair is attempted. The attachment is deleted from the message.
Log only	No repair is attempted. The incident of a virus is logged, and the message is delivered.

Table 1-4 shows options for handling unrepairable infected attachments.

Table 1-4 Options for handling unrepairable infected attachments

Option	Description
Delete	The attachment is deleted from the message.
Log only	The incident of a virus is logged, and the message is delivered.

Table 1-5 shows options for handling attachments that are not repaired or deleted.

Table 1-5 Options for handling attachments that are not repaired or deleted

Option	Description
Drop message	Emails containing unrepairable infected attachments that were not deleted are dropped.
Log only	A record of the incident is logged and the message is delivered.

Table 1-6 shows quarantine options for infected attachments.

Table 1-6 Quarantine options

Option	Description
Quarantine nothing	No files are quarantined.
Quarantine only unrepaired infections	Attachments that cannot be repaired are quarantined. **Note:** This option is available only if you have scanning enabled in Symantec AntiVirus for SMTP Gateways and it is configured to repair attachments.

Table 1-6 Quarantine options

Option	Description
Quarantine all infections	All infected attachments are quarantined. **Note:** This option is available only if you have scanning enabled in Symantec AntiVirus for SMTP Gateways.

Set antispam controls

Symantec AntiVirus for SMTP Gateways can be configured to do the following:

- Use Domain Name Server black lists (DNSBL) to keep spam from being relayed through your network.

  You can create an antispam white list to let email from certain domains bypass spam processing.
- Block email based on characters (most often, % and !) that often appear in email addresses that are associated with spam relaying.
- Activate the heuristic spam engine to detect spam.

See “Blocking spam” on page 76.

Configure relay settings

Symantec AntiVirus for SMTP Gateways works in conjunction with email software products that are running on other local mail servers. After processing email, Symantec AntiVirus for SMTP Gateways relays the email to mail servers according to how you have configured your relay settings.

See “Configuring routing options” on page 54.

By establishing anti-relay settings, Symantec AntiVirus for SMTP Gateways prevents the relaying of spam by an external host.

See “Preventing spam relaying” on page 81.

Notify senders and administrators of policy violations

Symantec AntiVirus for SMTP Gateways lets you customize notifications for administrators and senders when any of the following occur:

- Infected attachment
- Virus outbreak
- Content violation
- Exceeded container limit
- Deleted encrypted container
- Domain Name Server black list (DNSBL) antispam list violation
- System events
- Block by sender address

Chapter 2

Installing Symantec AntiVirus for SMTP Gateways

This chapter includes the following topics:

Before you install

You must perform the following pre-installation tasks when appropriate:

- Install and configure the operating system.
  See "Installing and configuring the operating system" on page 22.
- Upgrade from earlier versions of Symantec AntiVirus for SMTP Gateways.
  See "Upgrading from earlier versions" on page 22.
- Configure DNS.
  See "Configuring DNS" on page 23.
- Prevent conflicts with other SMTP servers.
  See "Preventing conflicts with other SMTP servers" on page 24.
- Prevent conflicts with other software.
  See "Preventing conflicts with other software" on page 24.
- Prevent conflicts with Symantec Web Security.
  See "Preventing conflicts with Symantec Web Security" on page 25.

Installing and configuring the operating system

Your server's operating system software and applicable updates must be installed, configured, and working correctly before you install Symantec AntiVirus for SMTP Gateways. Consult your server's documentation for more information. Installation of your operating system software and updates is outside the scope of this guide.

Upgrading from earlier versions

To upgrade from Symantec AntiVirus for SMTP Gateways 3.0, install version 3.1 on top of the existing software. This allows you to retain settings from the previous version.

Note: When Symantec AntiVirus for SMTP Gateways 3.1 is installed over a previous version, spam sender domains that do not begin with @ or a period are deleted from the configuration file. If you copy the configuration file prior to upgrading, you can edit the entries to begin with @ or a period.

Symantec AntiVirus for SMTP Gateways uses configuration files that may conflict with Norton AntiVirus™ for Gateways. If you have Norton AntiVirus for Gateways 2.5.2 installed, you must first install Symantec AntiVirus for SMTP

Gateways, and then uninstall Norton AntiVirus for Gateways. Doing so lets you retain settings from the previous product. If you have an earlier version than Norton AntiVirus for Gateways 2.5.2 installed, you must first uninstall that version, and then perform a clean installation of Symantec AntiVirus for SMTP Gateways.

There may be files and registry entries that are not removed when Norton AntiVirus for Gateways is uninstalled. You must manually delete these files and entries.

Configuring DNS

Symantec AntiVirus for SMTP Gateways works in conjunction with other SMTP mail servers. By properly configuring your site's DNS, email that is destined for your existing mail server arrives at Symantec AntiVirus for SMTP Gateways first. After scanning for viruses, Symantec AntiVirus for SMTP Gateways forwards the email to your SMTP server for delivery.

The DNS zone for your site must be configured to support Reverse Name Lookup, which is used to verify the IP address of the host or domain that you are trying to resolve.

Symantec AntiVirus for SMTP Gateways processing is affected when you modify DNS records. There are two types of records that are involved in the delivery of email:

- A record: A mapping of host name to IP address. For example, the host name www.somewhere.com might map to the specific IP address 192.168.23.10.
- MX record: A mapping of domains to mail exchange host names. Any email that is sent to a particular user at a domain (such as user@somewhere.com) is resolved by a DNS server MX record to a host name, such as mailer.somewhere.com. Then the A record resolves the name mailer.somewhere.com to an IP address.

By adding a higher priority MX record for the Symantec AntiVirus for SMTP Gateways host, all email that is destined for the mail server arrives at Symantec AntiVirus for SMTP Gateways first. After processing, Symantec AntiVirus for SMTP Gateways forwards the email to the mail server for delivery.

Consult with your network administrator or Internet service provider (ISP) if you are unsure of how to configure DNS records.

Note: You may also choose to modify DNS so that the MX record points to the firewall, in which case the firewall would route traffic internally. In this scenario, changes are made to the firewall rather than to the MX record.

Preventing conflicts with other SMTP servers

Because Symantec AntiVirus for SMTP Gateways is an SMTP server, it must have exclusive access to the TCP/IP port that corresponds to that service. No other SMTP servers can be running on the same port on the same server on which Symantec AntiVirus for SMTP Gateways is installed. You must disable these conflicting services prior to installing Symantec AntiVirus for SMTP Gateways.

Note: When you install Symantec AntiVirus for SMTP Gateways on a Solaris™ server, the installation program may detect conflicting programs that are commonly found on Solaris (such as the Solaris Sendmail™ program being run on port 25). If such programs are detected, the installation program will issue a warning and offer to disable these programs automatically. Although reasonable effort has been made to make the automatic disabling of these conflicting programs safe, the attempt may still fail, possibly leaving your server in an uncertain condition. Therefore, you may want to disable the conflicting programs prior to installing Symantec AntiVirus for SMTP Gateways.

Preventing conflicts with other software

Warning: If you are running a desktop antivirus product on the server on which you will install Symantec AntiVirus for SMTP Gateways, you must configure the desktop product not to scan the temporary directory that will be used by Symantec AntiVirus for SMTP Gateways.

You must disable any other antivirus software on the server on which Symantec AntiVirus for SMTP Gateways will be installed. After installation, reenable the antivirus protection.

If another antivirus product is installed on the Symantec AntiVirus for SMTP Gateways server, the competing product may try to scan and delete Symantec AntiVirus for SMTP Gateways files that are placed in the temporary directory during its scanning process.

Preventing conflicts with Symantec Web Security

If you are running Symantec Web Security and Symantec AntiVirus for SMTP Gateways on the same computer, install Symantec AntiVirus for SMTP Gateways, and then disable LiveUpdate in Symantec AntiVirus for SMTP Gateways.

See "To schedule Automatic LiveUpdate" on page 91.

Once the latest antivirus update is downloaded to your server, it is shared by both applications. This may cause conflicts when you download updates to both applications if LiveUpdate is not disabled in Symantec AntiVirus for SMTP Gateways.

System requirements

You need root or administrator-level privileges to install Symantec AntiVirus for SMTP Gateways. You should install Symantec AntiVirus for SMTP Gateways on its own server.

The minimum system requirements for Solaris and Windows NT/2000 Server are as follows:

- Solaris: SPARC®-based server

  Windows NT/2000 Server: Intel® Pentium® or compatible
- Solaris version 7.0 or 8.0

  Windows NT 4.0 with Service Pack 3 or later, or Windows 2000 Server with Service Pack 2
- 256 MB RAM (512 MB or more recommended for optimal performance)
- 50 MB to install (500 MB minimum after installation for email processing)
- Static IP address for the computer that will run Symantec AntiVirus for SMTP Gateways
- TCP/IP Internet connection
- Appropriately configured DNS, to include Address (A), Pointer (PTR), and Mail eXchange (MX) records for your servers
- DNS zone for your site that is configured to support Reverse Name Lookup
- Netscape Navigator version 4.75 or later, or Microsoft Internet Explorer version 5.0 or later

Installing Symantec AntiVirus for SMTP Gateways

Note: You should install Symantec AntiVirus for SMTP Gateways on a separate server from your SMTP server so that there is no significant impact on network resources.

You need root or administrator-level privileges to install Symantec AntiVirus for SMTP Gateways. A static IP address is required.

If you decide to install Symantec AntiVirus for SMTP Gateways on the same computer that your SMTP server is on, you must configure Symantec AntiVirus for SMTP Gateways to listen on a port other than the one on which your SMTP server listens. Since port 25 is the port to which most servers send email connection requests, you will most likely want to have Symantec AntiVirus for SMTP Gateways listen on port 25. If your SMTP server is currently listening on port 25, you must change your server to listen on a different port.

On Solaris, if another process is running on port 25, Symantec AntiVirus for SMTP Gateways attempts to automatically disable it. A record that the process has been disabled is placed in the log directory. If another process is disabled because it is running on port 25, there is an on-screen option during installation that lets you stop the installation process and change the port for the existing process or allow Symantec AntiVirus for SMTP Gateways to disable the process and continue the installation on port 25.

Note: If another process that is running on port 25 is disabled, you must configure the disabled software to run on another port.

Complete the following tasks in the order in which they are listed to install Symantec AntiVirus for SMTP Gateways:

- Verify that DNS is properly configured for your network.
  See "Verifying DNS on the Symantec AntiVirus for SMTP Gateways server" on page 27.
- Run the install script or setup program to install.
  See "Running the install script or setup program" on page 28.
- Specify locations for install directories.
  See "Specifying locations for installation directories" on page 29.

- Select an HTTP server port.
  See "Selecting an HTTP server port" on page 31.
- Select an HTTPS server port.
  See "Selecting an HTTPS server port" on page 32.

Verifying DNS on the Symantec AntiVirus for SMTP Gateways server

Your server must be configured as a DNS client prior to installing Symantec AntiVirus for SMTP Gateways.

Verify and test your DNS settings

To verify your DNS settings, you must check your TCP/IP properties. To test your DNS server, use the Name Server Lookup (NSLookup) utility.

To verify your DNS settings on Windows 2000 Server

1. Open Local Area Connection Properties.
2. Click **Internet Protocol** (**TCP/IP**).
3. Click **Properties**.
4. Click **Advanced**.
5. On the DNS tab, specify the domain suffix and verify that at least one valid DNS server is listed in the DNS server addresses list.
   The host name is the Computer name that is entered in System Properties on the Network Identification tab.

Consult with your network administrator or Internet service provider (ISP) if you are unsure of the values to use.

To verify your DNS settings on Windows NT

1. Open the Network control panel.
2. On the Protocols tab, click **TCP/IP Protocol**.
3. Click **Properties**.
4. In the TCP/IP Properties window, click **DNS**.
5. Verify that the Host Name and Domain boxes contain the correct values, and that at least one valid DNS server is listed in the DNS Service Search Order list.

To verify your DNS settings on Solaris

1. Open the following file:

   /etc/resolv.conf

   The file should contain lines similar to the following:

   ```
   domain somewhere.com
   nameserver 192.168.1.2
   nameserver 192.168.9.7
   ```

   Verify that the specific domain name and name server addresses that are used in your file are correct for your site.

   Consult with your network administrator or Internet service provider (ISP) if you are unsure of the values to be used.

2. Make any necessary changes.

If the /etc/resolv.conf file does not exist on your server, create it using the above example as a template. Replace the domain name and name server addresses with values that are correct for your site.

To test your DNS server

◆ Run the NSLookup command in the following format:

  ```
  nslookup <IP address or server name>
  ```

  For example, nslookup 155.55.55.55

The IP address should resolve to your server name and the server name should resolve to your IP address.

Note: You should run NSLookup twice (once in the format “nslookup <host name>” and once as “nslookup <IP address>”).

Running the install script or setup program

You must run the install script (Solaris) or setup program (Windows NT/2000 Server) to install Symantec AntiVirus for SMTP Gateways.

Run the install script or setup program

For Solaris, you must be logged on as root. The Symantec AntiVirus for SMTP Gateways files are on the CD.

For Windows NT/2000 Server, you must be logged on with administrator privileges. The Symantec AntiVirus for SMTP Gateways files are on the CD.

To install Symantec AntiVirus for SMTP Gateways on Solaris

1. Change (cd) to the location of the installation files.
2. Type the following command to run the install script:

   sh savsmtp.sh
3. Follow the on-screen directions.

   A transcript of the installation is saved as /var/log/SAVSMTP-install.log for later review, if necessary.
4. Verify that the software is running by viewing the Status page.

   The Date server started field should be current.

   See "About the Status page" on page 94.

To install Symantec AntiVirus for SMTP Gateways on Windows NT/2000 Server

1. Change (cd) to the location of the installation files.
2. Run Setup.exe.
3. Follow the on-screen directions.
4. Verify that the software is running by viewing the Status page.

   The Date server started field should be current.

   See "About the Status page" on page 94.

Specifying locations for installation directories

Symantec AntiVirus for SMTP Gateways is organized into directories that each contain specific kinds of files.

The location of each directory can be specified during installation, during which a default location is shown. Unless you have a compelling reason to do otherwise, you should accept the default location.

Table 2-1 shows the default installation directory locations for Solaris.

Table 2-1 Installation directories for Solaris

Directory	Description	Default location
InstallDir	Contains the Symantec AntiVirus for SMTP Gateways program files and read-only data files. At least 5 MB disk space required.	/opt/SAVSMTP

Table 2-1 Installation directories for Solaris

Directory	Description	Default location
MailDir	Contains SMTP queue files. At least 500 MB disk space recommended.	/var/opt/SAVSMTP/queues
LocalDir	Contains server-specific configuration files. At least 1 MB disk space required.	/var/opt/SAVSMTP/local
LogDir	Contains log files that record Symantec AntiVirus for SMTP Gateways activity. At least 600 MB disk space recommended.	/var/opt/SAVSMTP/logs
DiagDir	Contains files that may help Symantec technicians address issues that may arise with the software. At least 34 MB disk space recommended.	/var/opt/SAVSMTP/queues/ diagnosticfiles
ScanDir	Contains temporary files that are created during Symantec AntiVirus for SMTP Gateways scanning. At least 100 MB disk space recommended. **Note:** Files in the ScanDir are deleted after scanning.	/tmp/savsmtptemp
DocsDir	Contains readme. At least 1 MB disk space recommended.	var/opt/SAVSMTP/manuals/ english

Table 2-2 shows the Windows default installation directory locations.

Table 2-2 Installation directories for Windows

Directory	Description	Default location
Install	Contains the Symantec AntiVirus for SMTP Gateways program files and read-only data files. At least 5 MB disk space required.	\ProgramFiles\Symantec \SAVSMTP
Queues	Contains SMTP queue files. At least 500 MB disk space recommended.	\ProgramFiles\Symantec \SAVSMTP\queues

Table 2-2 Installation directories for Windows

Directory	Description	Default location
Local	Contains server-specific configuration files. At least 1 MB disk space required.	\ProgramFiles\Symantec \SAVSMTP\local
Logs	Contains log files that record Symantec AntiVirus for SMTP Gateways activity. At least 600 MB disk space recommended.	\ProgramFiles\Symantec \SAVSMTP\logs
Diagnostic	Contains files that may help Symantec technicians address issues that may arise with the software. At least 34 MB disk space recommended.	\ProgramFiles\Symantec \SAVSMTP\queues\diagnostic files
Docs	Contains readme. At least 1MB disk space recommended.	\Program Files\Symantec\SAVSMTP\ docs\english

Selecting an HTTP server port

The Symantec AntiVirus for SMTP Gateways software is managed through a Web-based interface. This interface is provided through a built-in Hypertext Transfer Protocol (HTTP) server that is included with Symantec AntiVirus for SMTP Gateways. This HTTP server is independent of any existing HTTP server that already may be installed on your server and is not a general-purpose Web server.

During the installation process, you will be prompted for the TCP/IP port number on which this built-in HTTP server will listen. The number that you specify becomes the port number in the URLs you will use to access the Symantec AntiVirus for SMTP Gateways interface. The port number that is specified must be different from the HTTPS and SMTP port numbers, exclusive to Symantec AntiVirus for SMTP Gateways, and not already in use by any other program or service.

Because the built-in HTTP server is not a general-purpose Web server, do not use port number 80 (the default port number for general-purpose Web servers). Unless you have a compelling reason to do otherwise, you should use the default port number of 8003. If you select a port number other than the default, do not forget which port number you selected.

Selecting an HTTPS server port

HTTPS stands for HTTP via Secure Sockets Layer (SSL). With HTTP, all information is sent in clear text with no authentication between client and server. With HTTPS, there is client and server authentication via a certificate that has been signed by a Certificate Authority. Once a legitimate Web certificate is installed on Symantec AntiVirus for SMTP Gateways, the server and client now share a common key that lets them encrypt and decrypt messages that they send to each other. In Symantec AntiVirus for SMTP Gateways, secure connections are used for the logon- and password-changing portions of the administrative interface, when they are enabled.

During installation, you must identify the TCP/IP port number on which the HTTPS server will listen. The port number that you specify must be different from the HTTP and SMTP port numbers, exclusive to Symantec AntiVirus for SMTP Gateways, and not already in use by any other program or service. The default HTTPS port number is 8043. Unless you have a compelling reason to do otherwise, you should select the default.

Note: You must identify an HTTPS port number during installation even if you do not enable SSL.

Post-installation tasks

You must perform the following post-installation tasks when appropriate:

- Access the administrative interface.
  See "Accessing the administrative interface" on page 33.
- Route scanned email for delivery.
  See "Routing scanned email for delivery" on page 34.
- Stop and restart Symantec AntiVirus for SMTP Gateways.
  See "Stopping and restarting Symantec AntiVirus for SMTP Gateways" on page 34.

Accessing the administrative interface

You must access the administrative interface to configure Symantec AntiVirus for SMTP Gateways.

Access the Symantec AntiVirus for SMTP Gateways administrative interface

You can access Symantec AntiVirus for SMTP Gateways through a browser window, from the Start menu, or by clicking the desktop icon (if it is running on Windows).

To access the Symantec AntiVirus for SMTP Gateways administrative interface via a browser window

1. Open your browser.
2. Type the Symantec AntiVirus for SMTP Gateways IP address or host name in the following format:

   http://<IP address or host name of the computer that is running the software>:<port #>

   For example, use either of these formats:

   http://savsmtp.somewhere.com:8003

   http://198.0.0.1:8003
3. Log on using the password that you set during installation.

   Passwords are case sensitive.

To access the Symantec AntiVirus for SMTP Gateways administrative interface via the Start menu

1. On the Windows taskbar, click **Start** > **Programs**.
2. Click **Symantec AntiVirus for SMTP Gateways**.

Routing scanned email for delivery

Unless the Symantec AntiVirus for SMTP Gateways server is the last hop before the Internet, you must configure Symantec AntiVirus for SMTP Gateways to route scanned email to your mail hosts for delivery.

To route scanned email for delivery

1. Open Symantec AntiVirus for SMTP Gateways.
2. On the Symantec AntiVirus for SMTP Gateways administrative interface, in the left pane, click **Configuration**.
3. On the Routing tab, under Local Routing List, click **Add**.
4. Under Routing list entry, in the Host or Domain box, type the domain of your mail server (for example, brightcorp.com).
5. Under Destination relay, in the Host box, type the fully qualified domain name or IP address of your mail server.
6. In the Port box, type the port number of your mail server.
7. Click **Save**.

Note: You must add a routing list entry for each serviced email domain on your network.

All mail that was previously destined for your SMTP server goes to Symantec AntiVirus for SMTP Gateways for processing, then is forwarded to your SMTP server for delivery.

Stopping and restarting Symantec AntiVirus for SMTP Gateways

Warning: All of the files in the temporary directory are deleted at startup.

You may need to stop and restart Symantec AntiVirus for SMTP Gateways. Stopping and restarting the service results in a lost connection to client applications that may be submitting a file for scanning or delivery. The client application must reestablish the connection and resubmit the file for scanning and delivery.

Note: If messages are being processed when the service is stopped, the processing of those messages stops and resumes when the service is restarted.

Stop and restart Symantec AntiVirus for SMTP Gateways

Instructions for stopping and restarting Symantec AntiVirus for SMTP Gateways differ depending on the operating system that you are running. If you are running Symantec AntiVirus for SMTP Gateways on Windows NT/2000 Server, stop and restart service in the Services Control Panel.

To stop and restart Symantec AntiVirus for SMTP Gateways on Solaris

1. Stop the service by typing **/etc/rc2.d/S87savsmtp stop**.
2. Restart the service by typing # **/etc/rc2.d/S87savsmtp start**.

To stop and restart Symantec AntiVirus for SMTP Gateways on Windows

1. On the Windows taskbar, click **Start** > **Programs** > **Administrative Tools** > **Services.**
2. Right-click **Symantec AntiVirus for SMTP Gateways**, then click **Stop**.
3. Right-click **Symantec AntiVirus for SMTP Gateways**, then click **Start**.

Uninstalling Symantec AntiVirus for SMTP Gateways

There are different instructions for uninstalling Symantec AntiVirus for SMTP Gateways from Solaris and Windows.

Uninstall Symantec AntiVirus for SMTP Gateways from Solaris

There may be files and registry entries that are not removed when you uninstall Symantec AntiVirus for SMTP Gateways. You must manually delete those files and entries.

Warning: If you are running other Symantec antivirus products, certain shared files, including LiveUpdate and registry files, should not be deleted.

If Symantec AntiVirus for SMTP Gateways was permitted to automatically disable conflicting services when it was installed, an attempt will be made during uninstalling to reenable the services that were disabled during installation.

To uninstall Symantec AntiVirus for SMTP Gateways on Solaris

- ◆ Type the following command:
  pkgrm SYMCsmtp

To manually delete files and registry entries that are left behind after uninstalling

- Type the following commands:

  ```
  rm -r /var/opt/SAVSMTP
  rm -r /opt/Symantec
  rm -f /etc/Symantec.com
  rm -f /etc/symantec.reg
  rm -f /etc/liveupdate.conf
  rm -f /var/log/SYMANTEC.error
  rm -f /var/log/SAVSMTP-install.log
  ```

  These commands are based on default directory locations. If you changed the default directory locations, your commands will be different from those listed above.

Uninstall Symantec AntiVirus for SMTP Gateways from Windows NT/2000 Server

There may be files and registry entries that are not removed when you uninstall Symantec AntiVirus for SMTP Gateways. You must manually delete those files and entries.

To uninstall Symantec AntiVirus for SMTP Gateways from Windows

- Do one of the following:
  - In the Windows Control Panel, double-click **Add/Remove Programs**, click **Symantec AntiVirus for SMTP Gateways 3.1**, then click **Remove**.
  - From the Start menu, select **Programs** > **SAVSMTP** > **Uninstall SAVSMTP**.

To manually delete files left that are behind after uninstalling

1. Go to C:Program Files\Symantec\SAVSMTP.
2. Delete the **SAVSMTP** folder.
3. From the Add/Remove Programs list, delete LiveUpdate.

   Warning: If you are running other Symantec antivirus products, certain shared files, including LiveUpdate and registry files, should not be deleted.

To manually delete registry entries that are left behind after uninstalling

Warning: Do not delete registry events if you are running other Symantec products.

1 On the Windows taskbar, click **Start** > **Run**.

2 In the Run window, type **regedit**.

3 Click **OK**.

4 In the Registry Editor window, under My Computer, double-click **HKEY_LOCAL_MACHINE**.

5 Double-click **SOFTWARE**.

6 Right-click the **Symantec** folder, then click **Delete**.

7 In the Confirm Key Delete window, click **Yes**.

Chapter 3

Configuring Symantec AntiVirus for SMTP Gateways

This chapter includes the following topics:

Configuring administrator settings

There are two types of administrator accounts that can be set in Symantec AntiVirus for SMTP Gateways:

- Administrator: Oversees administration of Symantec AntiVirus for SMTP Gateways
- Report-only administrator: Has privilege to run reports on Symantec AntiVirus for SMTP Gateways only

Note: The report-only administrator password must be different from that of the administrator.

Configure administrator settings

Table 3-1 shows administrator settings that you can configure through the administrative interface.

Table 3-1 Administrator settings

Setting	Description
Administrator password	The administrator password is set during installation and can be changed through the administrative interface.
Report-only administrator password	The report-only administrator password can be set only through the administrative interface.
Administrator timeout	The administrator timeout applies to both the administrator and the report-only administrator accounts.
Administrator email addresses for notifications and alerts	The addresses to which notifications and alerts are sent when policy violations occur.

To change an administrator password through the administrative interface

1. On the Symantec AntiVirus for SMTP Gateways administrative interface, in the left pane, click **Configuration**.
2. On the Accounts tab, under Administration Passwords, under Administrator password, in the New password box, type a password for the administrator.

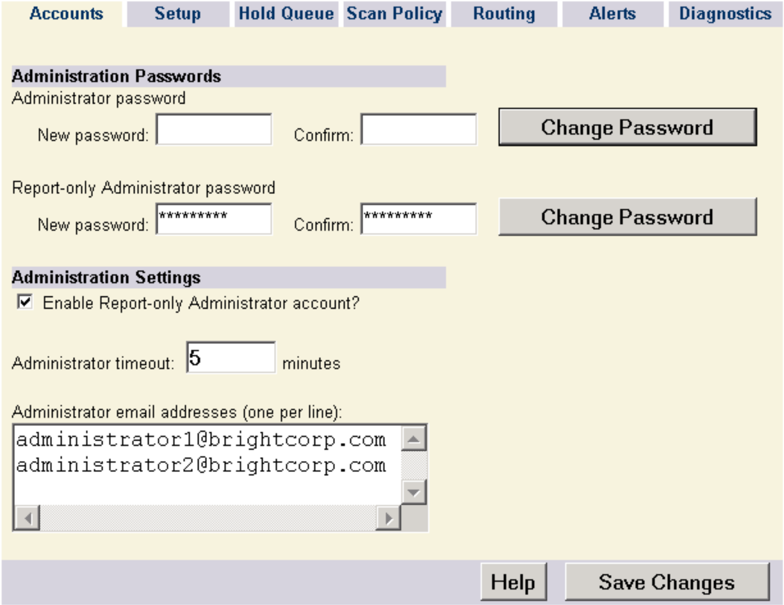
   Passwords are case sensitive.

   You do not need to set one through the interface unless you want to change the password you set during installation.

3. In the Confirm box, type the password again.
4. Click **Change Password**.

To set a report-only administrator password through the interface

1. On the Symantec AntiVirus for SMTP Gateways administrative interface, in the left pane, click **Configuration**.



Administration Passwords

Administrator password

New password: Confirm:

Report-only Administrator password

New password: ********** Confirm: **********

Administration Settings

☑ Enable Report-only Administrator account?

Administrator timeout: 5 minutes

Administrator email addresses (one per line):

administrator1@brightcorp.com
administrator2@brightcorp.com

2. On the Accounts tab, under Administration Passwords, under report-only Administrator password, in the New password box, type a password for the report-only administrator.

   Passwords are case sensitive.
3. In the Confirm box, type the password again.
4. Click **Change Password**.

To enable report-only administrator account

1. On the Symantec AntiVirus for SMTP Gateways administrative interface, in the left pane, click **Configuration**.
2. On the Accounts tab, under Administration Settings, check **Enable Report-only Administrator account**.
3. Click **Save Changes**.

Note: The report-only administrator password must be set before enabling the account.

To set the administrator timeout

1. On the Symantec AntiVirus for SMTP Gateways administrative interface, in the left pane, click **Configuration**.
2. On the Accounts tab, under Administration Settings, in the Administrator timeout box, type the number of minutes that will elapse without activity before a new logon is required.

   Five minutes is the default.

   The administrator timeout applies to both the administrator and the report-only administrator.
3. Click **Save Changes**.

To set administrator email addresses for notifications and alerts

1. On the Symantec AntiVirus for SMTP Gateways administrative interface, in the left pane, click **Configuration**.
2. On the Accounts tab, under Administration Settings, in the Administrator email addresses box, type the email addresses to which notifications and alerts will be sent.

   Type one email address per line.
3. Click **Save Changes**.

   In addition to setting an email address for notifications and alerts, you must configure Symantec AntiVirus for SMTP Gateways correctly to have it send notifications and alerts. This is done through the individual Notify and Alerts tabs.

Configuring connection and delivery options

You may configure the following in Symantec AntiVirus for SMTP Gateways:

- SMTP connection
  See "Configuring SMTP options" on page 43.
- Delivery options
  See "Configuring delivery options" on page 45.
- HTTP connection
  See "Configuring HTTP connection" on page 46.
- HTTPS connection
  See "Configuring HTTPS options" on page 47.
- Temporary directory location
  See "Changing the temporary files directory location" on page 49.

Configuring SMTP options

Note: You may not use the same port number for SMTP, HTTP, or HTTPS. To change more than one port number to a port number that is used by another application, you must change one port number at a time. If you change more than one port number at a time, and you switch, for example, the port number that is used for HTTP with the port number that is used for HTTPS, you will receive an error message because Symantec AntiVirus for SMTP Gateways recognizes those port numbers as already being in use.

SMTP options apply to the Symantec AntiVirus for SMTP Gateways server, which receives email for scanning and then forwards the email for delivery.

To configure SMTP settings

1. On the Symantec AntiVirus for SMTP Gateways administrative interface, in the left pane, click **Configuration**.

2. On the Setup tab, under SMTP, in the SMTP port number box, type the port number for the port on which the Symantec AntiVirus for SMTP Gateways listens.

   The default is 25.

   If the SMTP port is reset to another port, only email that arrives at the other port will be processed. If a port number is entered that is already used, the SMTP port number reverts to the previously assigned port number and a warning message is displayed.

3. On the Maximum number of outgoing connections drop-down list, select the number of simultaneous connects for outgoing email.

   The default is 30. Increasing the default increases resources required by the program and diminishes performance. Unless you have a compelling reason to do otherwise, accept the default.

   Additional connections are queued when the system is already processing the maximum number of connections that are allowed.

   Multiprocessor computers can effectively use more connections than single processors.

4. On the Maximum number of incoming connections menu, select the number of simultaneous connections for incoming email.

   The default is 15. Unless you have a compelling reason to do otherwise, accept the default.

   Setting the number of connections too high can slow processing. Additional connections are queued when the system is already processing the maximum number allowed.

5. In the Alert/Notification “From:” box, type the text that you want to appear in the From field when Symantec AntiVirus for SMTP Gateways notifications are sent.

   The default is Symantec_AntiVirus _for_SMTP_Gateways.

   Warning: Do not type an actual administrative email account name in the From field. Software logic prevents message looping due to bounces by dropping all email destined to this From account. This means that if you enter an email account name in the From field, all email destined for that account will be dropped.

6. Click **Save Changes**.

Configuring delivery options

During a virus outbreak, you may want to pause delivery of messages or reject incoming messages. You can also specify the number of days to attempt to deliver a message.

Configure delivery options

Follow these instructions to pause delivery, reject incoming messages, and set the number of days to attempt message delivery.

To pause delivery of messages

1. On the Symantec AntiVirus for SMTP Gateways administrative interface, in the left pane, click **Configuration**.
2. On the Setup tab, under Delivery, check **Pause message delivery**.

   While this is checked, messages are still received and placed in the fast queue, but no messages are delivered. Once it is unchecked, the stored messages are delivered as usual.
3. Click **Save Changes**.

To reject incoming messages

1. On the Symantec AntiVirus for SMTP Gateways administrative interface, in the left pane, click **Configuration**.
2. On the Setup tab, under Delivery, check **Reject incoming messages**.

   While this is checked, no incoming messages are accepted, and the sending server receives notification that the service is not available. Once it is unchecked, incoming messages are processed as usual.
3. Click **Save Changes**.

To set the number of days to attempt message delivery

1. On the Symantec AntiVirus for SMTP Gateways administrative interface, in the left pane, click **Configuration**.
2. On the Setup tab, under Delivery, on the Number of days drop-down list, select the number of days that Symantec AntiVirus for SMTP Gateways will attempt to deliver a message.

   Once a message cannot be delivered, it is sent to the slow queue where Symantec AntiVirus for SMTP Gateways continues to attempt delivery. If a message cannot be delivered after the set number of days, it is returned to the sender and deleted from the slow queue and from the system.
3. Click **Save Changes**.

Configuring HTTP connection

The Symantec AntiVirus for SMTP Gateways software is managed through a Web-based interface. This interface is provided through a built-in Hypertext Transfer Protocol (HTTP) server that is included with the software. This HTTP server is independent of any existing HTTP server that is already installed on your server and is not a general-purpose Web server.

The HTTP port number is set during installation, but it can be changed through the administrative interface.

To configure HTTP connection

1. On the Symantec AntiVirus for SMTP Gateways administrative interface, in the left pane, click **Configuration**.
2. On the Setup tab, under HTTP/HTTPS, in the HTTP port number box, type the port number on which the built-in HTTP server will listen.

   The number that you specify becomes the port number in the URLs that you will use to access the Symantec AntiVirus for SMTP Gateways administrative interface. The port number must be exclusive to Symantec AntiVirus for SMTP Gateways and must not already be in use by any other program or service.

   Because the built-in HTTP server is not a general purpose Web server, do not use port number 80 (the default port number for general-purpose Web servers). Unless you have a compelling reason to do otherwise, you should use the default port number of 8003. If you select a port number other than the default, do not forget which port number you selected.
3. Click **Save Changes**.

Configuring HTTPS options

During installation, you must identify the port number for your HTTPS server. You can define an HTTPS server connection between computers on your network and Symantec AntiVirus for SMTP Gateways for SSL encryption of passwords during logon sessions.

Note: You must have an SSL Web server certificate installed prior to enabling SSL encryption for logons.

Configure HTTPS options

You must do the following to configure HTTPS options:

- Generate an SSL certificate request.
- Submit the certificate request to a recognized Certificate Authority.
- Install the certificate that is returned from the Certificate Authority.
- Enable SSL encryption.

To generate an SSL certificate request

1. On the Symantec AntiVirus for SMTP Gateways administrative interface, in the left pane, click **Configuration**.
2. On the Setup tab, in the HTTPS port number box, type the port number of the HTTPS server.

   The default port number is 8043. The port number must be exclusive to Symantec AntiVirus for SMTP Gateways and must not already be in use by any other program or service.
3. Click **Certificate Management**.
4. In the Certificate Management window, under Request, in the Common Name box, type the IP address or resolvable host name of the computer that is running Symantec AntiVirus for SMTP Gateways (for example, smart.brightschool.com).

   Check the Web site of the Certificate Authority to which the request will be submitted to see if there are format restrictions. For example, some Certificate Authorities require a resolvable host name instead of an IP address. Some require that the state or province name be spelled out.
5. In the Organization box, type the name of your organization (for example, Bright School).

6 In the Organization Unit box, type your business's main function (for example, Education).

7 In the City/Locality box, type your city or locality.

8 In the State/Province box, type your state or province.

If you do not have a state or province, you must type something in this field.

9 On the Country/Region drop-down list, select your country or region.

10 In the E-mail Address box, type your email address.

The certificate will be sent to the email address that is entered in this box.

11 Click **Create Request**.

The certificate request is displayed in the Certificate Management Request window.

To submit the certificate request to a recognized Certificate Authority

1 In the Certificate Management Request window, copy the entire request, including the header and footer, to your clipboard or to a text file.

2 Click **OK**.

3 Submit the clipboard contents or the copied text file to a recognized Certificate Authority (for example, VeriSign®) by pasting it on the Certificate Authority's site, as they direct.

The Certificate Authority emails your certificate to the address that you typed on the Certificate Request page.

To install the returned certificate on Symantec AntiVirus for SMTP Gateways

1 Copy the entire certificate, including header and footer, received via email from the Certificate Authority.

2 On the Symantec AntiVirus for SMTP Gateways administrative interface, in the left pane, click **Configuration**.

3 On the Setup tab, under HTTP/HTTPS, click **Certificate Management**.

4 In the Certificate Management window, under Install, paste the copied certificate, including header and footer.

5 Click **Install Certificate**.

To enable SSL encryption

1. On the Symantec AntiVirus for SMTP Gateways administrative interface, in the left pane, click **Configuration**.
2. On the Setup tab, under HTTP/HTTPS, check **Enable SSL & encryption for logons**.
3. Click **Save Changes**.

   In the Certificate Management window, under Status, you should now see the following:

   - Date on which the private key was installed.

     This was done automatically when you generated your request.
   - Date on which the certificate was installed
   - Date on which the certificate expires

     Expiration information is displayed only when SSL is enabled.

Acting as your own Certificate Authority

If you are able to act as your own Certificate Authority, you need only install a valid certificate on Symantec AntiVirus for SMTP Gateways and enable SSL encryption for logons.

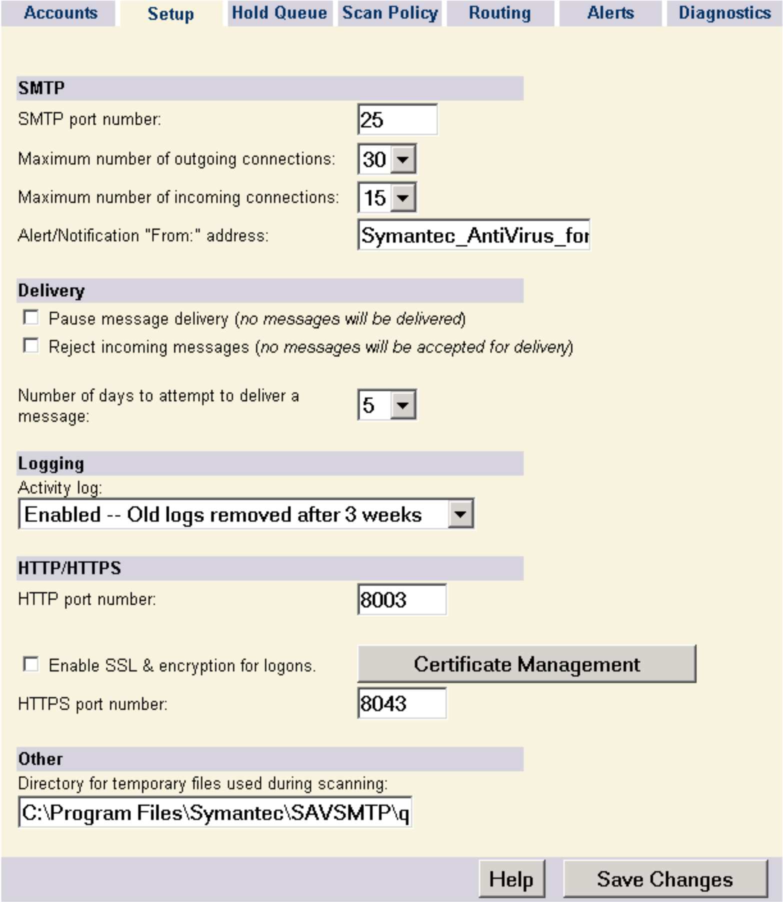
See "To install the returned certificate on Symantec AntiVirus for SMTP Gateways" on page 48 and "To enable SSL encryption" on page 49.

Changing the temporary files directory location

During installation, you select the locations for all directories. Through the administrative interface, you can change the location for the directories that contain temporary files created during Symantec AntiVirus for SMTP Gateways scanning.

To change the temporary files directory location

1 On the Symantec AntiVirus for SMTP Gateways administrative interface, in the left pane, click **Configuration**.



SMTP

SMTP port number: 25

Maximum number of outgoing connections: 30

Maximum number of incoming connections: 15

Alert/Notification "From:" address: Symantec_AntiVirus_for

Delivery

□ Pause message delivery (*no messages will be delivered*)

□ Reject incoming messages (*no messages will be accepted for delivery*)

Number of days to attempt to deliver a message: 5

Logging

Activity log: Enabled -- Old logs removed after 3 weeks

HTTP/HTTPS

HTTP port number: 8003

□ Enable SSL & encryption for logons.

HTTPS port number: 8043

Other

Directory for temporary files used during scanning: C:\Program Files\Symantec\SAVSMTP\q

2 On the Setup tab, under Other, in the Directory for temporary files used during scanning box, type the directory path where temporary files will be stored during scanning.

Windows default is \Program Files\Symantec\SAVSMTP\queues\Temp.

Solaris default is /tmp/savsmtptemp.

When a nondefault directory is set, a subdirectory names SAVSMTP is created in the nondefault location.

3 Click **Save Changes**.

Processing messages in the hold queue

Messages get into the hold queue in one of two ways:

- If a message causes a system crash three times, it is moved to the hold queue.
- If Symantec AntiVirus for SMTP Gateways is configured to hold messages that cannot be processed, those messages are sent to the hold queue.
  See "To configure scan options" on page 53.

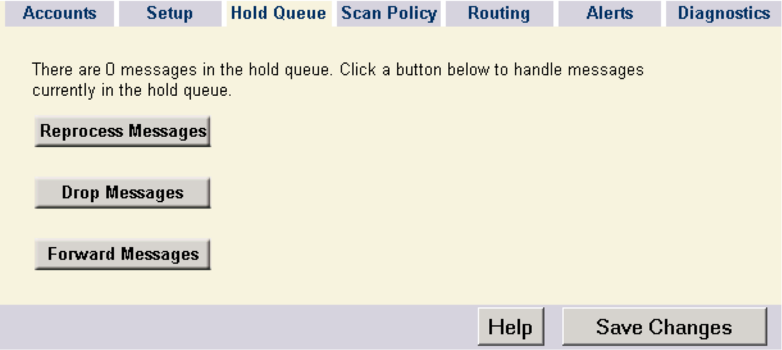
Process messages in the hold queue

You can configure Symantec AntiVirus for SMTP Gateways to reprocess, drop, or forward a copy of messages in the hold queue.

Warning: Reprocessing messages is not recommended. Reprocessing a message that has caused a system crash will likely result in another system crash.

To reprocess messages that are in the hold queue

1. On the Symantec AntiVirus for SMTP Gateways administrative interface, in the left pane, click **Configuration**.



There are 0 messages in the hold queue. Click a button below to handle messages currently in the hold queue.

2. On the Hold Queue tab, click **Reprocess Messages**.
3. In the Reprocessing Hold Queue Messages window, click **Yes**.
   All messages that are in the hold queue are reprocessed.

To drop messages that are in the hold queue

1. On the Symantec AntiVirus for SMTP Gateways administrative interface, in the left pane, click **Configuration**.
2. On the Hold Queue tab, click **Drop Messages**.
3. In the Dropping Hold Queue Messages window, click **Yes**.

   All messages that are in the hold queue are dropped from your system and are not delivered.

To forward messages that are in the hold queue

1. On the Symantec AntiVirus for SMTP Gateways administrative interface, in the left pane, click **Configuration**.
2. On the Hold Queue tab, click **Forward Messages**.
3. In the Forwarding Hold Queue Messages window, click **Yes**.
4. In the Subject box, type the subject for the forwarded email messages.
5. In the Email address box, type one email address to which emails in the hold queue are to be forwarded.
6. Click **Forward**.

   Copies of messages in the hold queue are forwarded. Copies are not scanned. Originals remain in the hold queue until they are dropped or manually deleted.

Configuring scan options

Part of setting your antivirus policy is setting a scan policy (determining what types of files are to be scanned and how to handle files that cannot be processed). By default, all files are scanned regardless of extension. For maximum security, do not change the default setting.

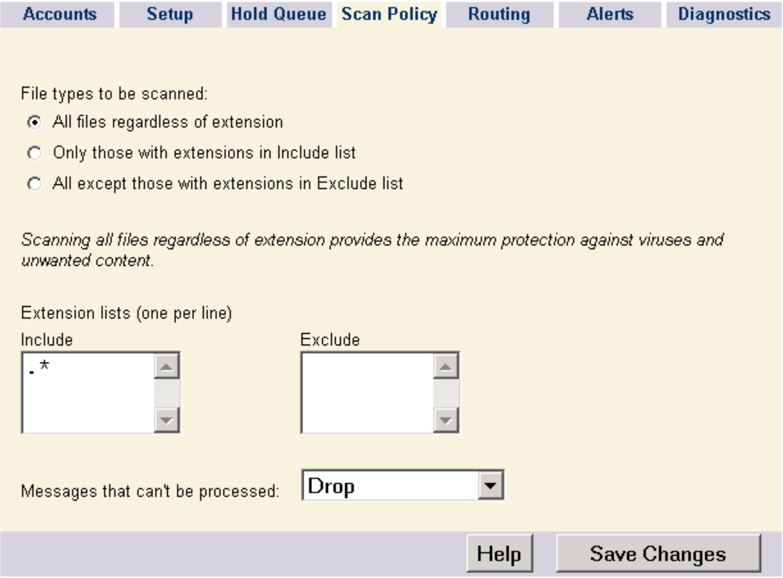
However, processing efficiency may be increased by identifying specific file types to scan. You can specify in the Include list those file types that are commonly at risk of infection. If the Include list includes .zip and .exe but not .cmd, and a container file, for example, test.zip, contains test.exe and test.cmd, only test.exe is scanned.

The Exclude list can be used to identify file types that are unlikely to carry viruses, for example, .gif, .jpeg, or .jpg.

Note: If a container file is included in the Exclude list, no files within it are scanned. For example, if .zip is listed in the Exclude list, and a .zip file that contains infected .com files is received, neither the .zip file nor the infected .com files will be scanned.

To configure scan options

1. On the Symantec AntiVirus for SMTP Gateways administrative interface, in the left pane, click **Configuration.**



File types to be scanned:
● All files regardless of extension
○ Only those with extensions in Include list
○ All except those with extensions in Exclude list

Scanning all files regardless of extension provides the maximum protection against viruses and unwanted content.

Extension lists (one per line)
Include: .*
Exclude:

Messages that can't be processed: Drop

2. On the Scan Policy tab, select one of the following:
   - All files regardless of extension
   - Only those with extensions in Include list
   - All except those with extensions in Exclude list

3 If Only those with extensions in Include list or All except those with extensions in Exclude list is selected, in the appropriate box, type one extension per line in the following format:

.ttt

Extensions are not case sensitive.

4 On the Messages that can't be processed drop-down list, select one of the following:

- Deliver
- Drop

  You should drop messages that cannot be processed. Most messages that cannot be processed have malformed MIME formatting or corrupted content that cannot be expanded for scanning.
- Bounce to sender
- Hold

5 Click **Save Changes**.

Configuring routing options

After it scans for viruses, Symantec AntiVirus for SMTP Gateways routes email to your existing hosts for delivery. There are two routing configurations:

- Default routing

  See "Configuring default routing" on page 54.
- Local routing

  See "Configuring local routing" on page 55.

Configuring default routing

Setting default routing is not required in most environments but must be done if no local routing is set.

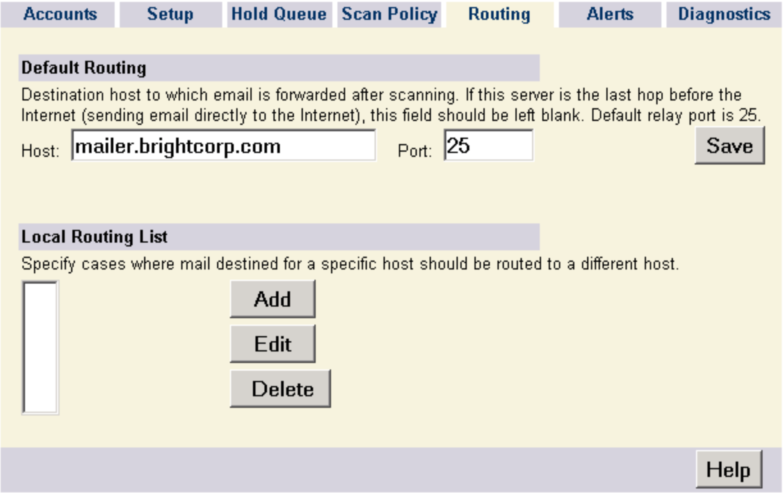
See "Preventing spam relaying" on page 81.

If the Default Routing box is filled in, any email that is not addressed to a host or domain in the Local Routing list (a name by itself or the name on the left side of an arrow) will be forwarded to the server on your network that is listed in the Default Routing box.

If this box is not filled in, any email that is not addressed to a name in the Local Routing list will be delivered to the appropriate SMTP server on the Internet.

To configure default routing

1 On the Symantec AntiVirus for SMTP Gateways administrative interface, in the left pane, click **Configuration**.



Default Routing

Destination host to which email is forwarded after scanning. If this server is the last hop before the Internet (sending email directly to the Internet), this field should be left blank. Default relay port is 25.

Host: mailer.brightcorp.com Port: 25

Local Routing List

Specify cases where mail destined for a specific host should be routed to a different host.

2 On the Routing tab, under Default Routing, in the Host box, type the fully qualified host name or IP address of your mail server.

3 In the Port box, type the port number of your mail server.
The default port number is 25.

4 Click **Save**.

Mail that was destined for your SMTP server goes to Symantec AntiVirus for SMTP Gateways for processing, and then is forwarded to the specified SMTP server for delivery.

Configuring local routing

Note: You must set a routing list entry for each email domain on your network with the domain (for example, brightcorp.com) as the Routed host or domain and your mail server as the Destination relay.

Setting local routing is required in most environments, and is essential if you are not using default routing. The typical setting for most environments is an email domain routed to an SMTP server.

The local routing list has two purposes:

- It defines special rules for relaying scanned email.
- It identifies which domains and hosts are considered local.

There are two types of local routing entries:

- A name by itself

  A name by itself means that Symantec AntiVirus for SMTP Gateways treats email addressed to that host name, domain, or IP address as local and does a DNS lookup for the address and delivers it where the MX record tells it to.

- A name followed by another name

  A name followed by another name means that when Symantec AntiVirus for SMTP Gateways receives and processes email addressed to the host name, IP address, or domain of the first mail server that it should use the second name to relay the mail.

  For example, if you type brightcorp.com in the Routed host or domain box and mailer.brightcorp.com in the Destination relay box, after Symantec AntiVirus for SMTP Gateways processes email addressed to brightcorp.com (user@brightcorp.com), it forwards the email to mailer.brightcorp.com for delivery.

In both cases, the first (or only) name is considered local. The second name (if any) is not. Local routing rules always have priority over the Default Routing setting.

Designating a host as local is significant for the relay restrictions.

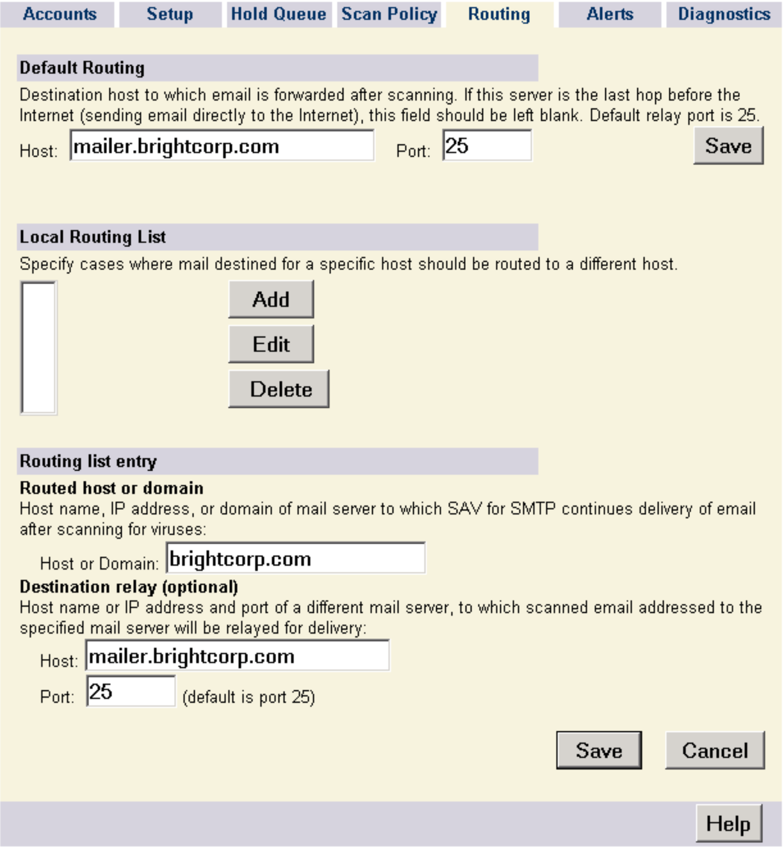
See “Preventing spam relaying” on page 81.

Configure local routing

You can create, edit, and delete local routing list entries.

To create local routing entries

1 On the Symantec AntiVirus for SMTP Gateways administrative interface, in the left pane, click **Configuration**.



Default Routing

Destination host to which email is forwarded after scanning. If this server is the last hop before the Internet (sending email directly to the Internet), this field should be left blank. Default relay port is 25.

Host: mailer.brightcorp.com Port: 25

Local Routing List

Specify cases where mail destined for a specific host should be routed to a different host.

Routing list entry

Routed host or domain

Host name, IP address, or domain of mail server to which SAV for SMTP continues delivery of email after scanning for viruses:

Host or Domain: brightcorp.com

Destination relay (optional)

Host name or IP address and port of a different mail server, to which scanned email addressed to the specified mail server will be relayed for delivery:

Host: mailer.brightcorp.com

Port: 25 (default is port 25)

2 On the Routing tab, under Local Routing List, click **Add**.

3 Under Routing list entry, type the host name, IP address, or domain of a mail server to which email should be routed.

Wildcard characters may be used in routing list entries.

If you type only the first entry and no destination relay, email that is addressed to a user who receives mail at that host will be relayed using that host.

4 Under Destination relay, in the Host box, type the host name, IP address, or domain of the mail server to which email that is destined for the server that is designated above should be routed.

If you type a destination host, email addressed to a user receiving mail at the host listed under Routed host or domain will be relayed using the host typed in the Host box under Destination relay.

5 In the Port box, type the port number for the mail server.

The default port number is 25.

6 Click **Save**.

To edit a local routing list entry

1 On the Symantec AntiVirus for SMTP Gateways administrative interface, in the left pane, click **Configuration**.

2 On the Routing tab, under Local Routing List, select the case that you want to edit.

3 Click **Edit**.

4 Make the changes that you want.

5 Click **Save**.

To delete a local routing list entry

1 On the Symantec AntiVirus for SMTP Gateways administrative interface, in the left pane, click **Configuration**.

2 On the Routing tab, under Local Routing List, select the case you want to delete.

3 Click **Delete**.

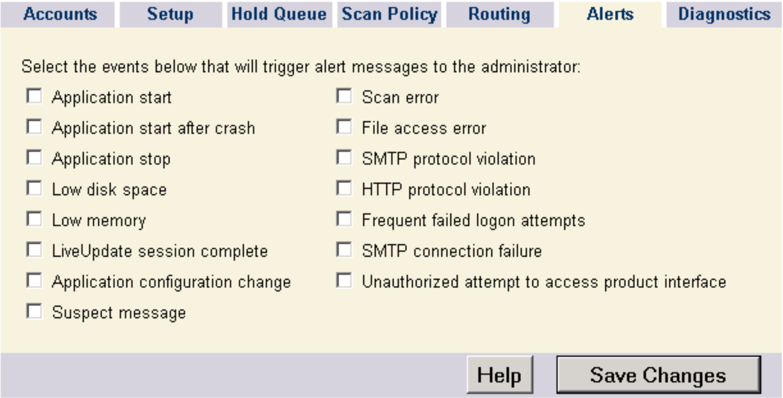
Configuring alerts

You can configure Symantec AntiVirus for SMTP Gateways to send alerts to one or more administrators for system events.

Note: If no email address is specified, alerts will not be delivered.
See “To set administrator email addresses for notifications and alerts” on page 42.

To configure alerts

1 On the Symantec AntiVirus for SMTP Gateways administrative interface, in the left pane, click **Configuration**.



Select the events below that will trigger alert messages to the administrator:

□ Application start
□ Application start after crash
□ Application stop
□ Low disk space
□ Low memory
□ LiveUpdate session complete
□ Application configuration change
□ Suspect message
□ Scan error
□ File access error
□ SMTP protocol violation
□ HTTP protocol violation
□ Frequent failed logon attempts
□ SMTP connection failure
□ Unauthorized attempt to access product interface

2 On the Alerts tab, select the events that will trigger alerts to the administrator.

The alerts will be sent to the email addresses that you designated when configuring administrative settings.

3 Click **Save Changes**.

Table 3-2 shows system events that trigger alerts, their descriptions, and examples of alerts.

Table 3-2 Events that trigger alerts

Event	Description	Alert text
Application start	The application has started.	Subject: Application Start Body: The application has been started.
Application start after crash	The server has started after an unexpected shutdown.	Subject: Application Start after Crash Body: The server has been started after an unexpected shutdown.
Application stop	The server has stopped.	Subject: Application Stop Body: The application has been stopped.

Table 3-2 Events that trigger alerts

Event	Description	Alert text
Low disk space	The disk space in the logging, email scanning, or mail queuing directory is less than 10%.	Subject: Low Disk Space Threshold Exceeded Body: The [ ] directory is running dangerously low on disk space, where [ ] is either logging, email, or mail queuing.
Low memory	Less than 10% of memory remains.	Subject: Low Memory Threshold Exceeded Body: The memory available on the server is running dangerously low.
LiveUpdate session complete	LiveUpdate has successfully completed a virus definitions update.	Subject: LiveUpdate Completed Body: The system completed a LiveUpdate operation.
Application configuration change	The software has been reconfigured in some way.	Subject: Configuration Change Body: A configuration change was made.
Suspect message	On the third attempt to send a message that crashes Symantec AntiVirus for SMTP Gateways or a message that triggers a "Cannot Scan" error, the message is considered suspect and moved to the hold queue.	Subject: Suspect Message Body: A suspect message was received by the server.
Scan error	The engine that handles decomposition of files has encountered an error during scanning.	Subject: Decomposition error Body: An error occurred during message decomposition.
File access error	A user has attempted to access a file for which the user has no permissions, or a file has been altered and, therefore, cannot be accessed.	Subject: File Access Error Body: A file access error occurred on the server.

Table 3-2 Events that trigger alerts

Event	Description	Alert text
SMTP protocol violation	During authentication, a protocol violation between SMTP servers has been detected.	Subject: SMTP Protocol Violation Body: An SMTP protocol violation was detected by the server.
HTTP protocol violation	During authentication, a protocol violation with the HTTP server has been detected.	Subject: HTTP Protocol Violation Body: An HTTP protocol violation was detected by the server.
Frequent failed logon attempts	Three unsuccessful logon attempts have been made. An alert is sent on the third attempt, and one is sent for every unsuccessful attempt thereafter. The counter is reset upon correct logon.	Subject: Frequent Failed Logon Attempts Body: Several failed logon attempts have been made to the server.
SMTP connection failure	The SMTP server that Symantec AntiVirus for SMTP Gateways is trying to contact is not available.	Subject: SMTP Connection Failure Body: A connection failure was encountered by the server.
Unauthorized attempt to access product interface	Users, including Report-only administrators, have attempted to access the administrative interface without appropriate permissions.	Subject: Unauthorized Attempt to Access Product Interface Body: An unauthorized attempt to access the server interface was detected.

Configuring logging options

There are two types of logging available in Symantec AntiVirus for SMTP Gateways: local logging and SESA logging. Local logging (logging of activity to the computer on which Symantec AntiVirus for SMTP Gateways is running) is enabled by default. For local logging, you can specify how long old logs should be retained, from one week to Never delete.

SESA logging (logging of activity to the SESA Console) is not enabled by default.

See "To configure logging options" on page 63 and "Integrating Symantec AntiVirus for SMTP Gateways with SESA" on page 109.

Once enabled, Symantec AntiVirus for SMTP logs the following local events to SESA:

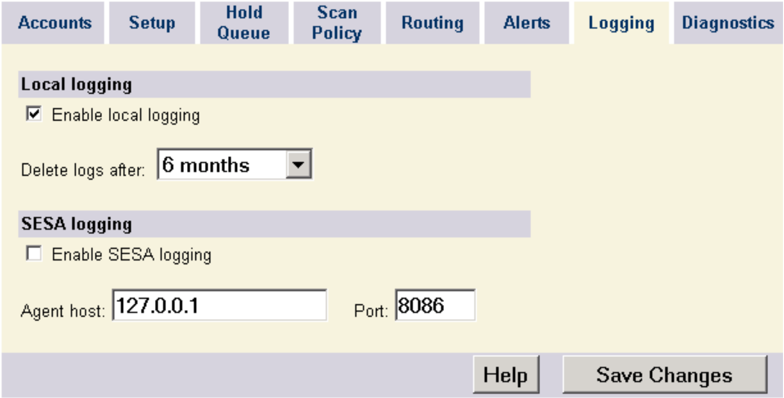
- Logon
- Logoff
- Definitions updated
- Object modified
- Protocol violation
- Messages rejected
- Messages dropped
- Messages bounced
- Delivery failed
- Virus logged
- Files repaired
- Files deleted
- Subjects blocked
- Scan error
- Sender blocked
- Attachment deleted
- Spam list block
- Heuristic spam detection
- Message statistics

See "Generating detail reports" on page 103.

Since no data is being retained while logging is disabled, it is impossible to generate reports on that data.

To configure logging options

1 On the Symantec AntiVirus for SMTP Gateways administrative interface, in the left pane, click **Configuration**.



Local logging

☑ Enable local logging

Delete logs after: 6 months

SESA logging

□ Enable SESA logging

Agent host: 127.0.0.1 Port: 8086

2 On the Logging tab, under Local logging, check or uncheck Enable local logging.

3 On the Delete logs after pull-down menu, select the time period to retain log files.

4 Under SESA logging, check or uncheck Enable SESA logging.

5 In the Agent host box, type the IP address on which the Agent listens.

6 In the Port box, type the port number on which the Agent listens.

7 Click **Save Changes**.

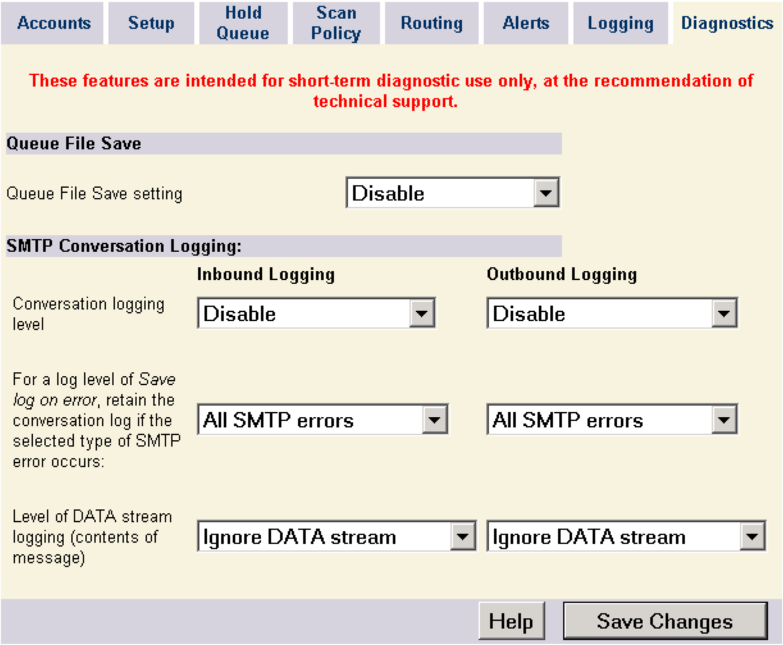
Configuring queue file save and SMTP conversation logging

Diagnostic files are located on Windows in the queues folder and on Solaris in the DiagDir. If you contact Symantec Technical Support for assistance, you may be instructed to configure the Queue File Save setting.

Warning: The default for the Queue File Save setting is Disable. Do not change this setting unless you are instructed by Symantec Technical Support to do so. Changing the setting can result in undesirable system behavior.

To configure queue file save

1. On the Symantec AntiVirus for SMTP Gateways administrative interface, in the left pane, click **Configuration**.
2. On the Diagnostics tab, under Queue File Save, on the Queue File Save setting drop-down list, select the setting that Symantec Technical Support tells you to select.
3. Click **Save Changes**.



These features are intended for short-term diagnostic use only, at the recommendation of technical support.

Queue File Save

Queue File Save setting: Disable

SMTP Conversation Logging:

	Inbound Logging	Outbound Logging
Conversation logging level	Disable	Disable
For a log level of *Save log on error*, retain the conversation log if the selected type of SMTP error occurs:	All SMTP errors	All SMTP errors
Level of DATA stream logging (contents of message)	Ignore DATA stream	Ignore DATA stream

Configuring SMTP conversation logging

Warning: The default for the SMTP Conversation Logging is Disable. Do not change this setting unless you are instructed by Symantec Technical Support to do so.

You can now configure SMTP protocol conversation logging (log the incoming and/or outgoing SMTP protocol conversation when accepting or delivering a message). If inbound logging is enabled, one conversation log is generated for each inbound connection. If outbound logging is enabled, one log is generated for each message delivery attempt.

Note: Conversation log files are saved to the diagnostic files directory defined during installation (default location is <InstallDir>/queues/diagnosticfiles, where <InstallDir> is the path of the top-level installation directory, such as var/opt/SAVSMTP or C:\Program Files\Symantec\SAVSMTP.

To configure conversation logging

1. On the Symantec AntiVirus for SMTP Gateways administrative interface, in the left pane, click **Configuration**.
2. On the Diagnostics tab, under SMTP Conversation Logging, on the logging drop-down lists, choose one of the following for the conversation logging level:
   - Disable

     No conversation logging is performed.
   - Save log on error

     Conversation logs are saved only if an SMTP error occurs during the message transmission.
   - Log all inbound (or outbound) traffic.

     All conversation logs are saved for inbound and/or outbound conversations.
3. On the Diagnostics tab, under SMTP Conversation Logging, on the logging drop-down lists, choose one of the following to determine error type triggers:
   - All SMTP errors

     All SMTP errors are logged.
   - Communication error

     Network and socket errors are logged.
   - Protocol error

     Failures to follow defined SMTP protocols (such as a command out of sequence or bad syntax) are logged.
   - Local processing error

     Application-defined errors (such as a message that exceeds defined size limits) are logged.
   - Unsupported operation

     Requests for unsupported operations (such as TURN) are logged.

4 On the Diagnostics tab, under SMTP Conversation Logging, on the logging drop-down lists, choose one of the following to determine the level of DATA stream logging:

- Ignore DATA stream
  Only the DATA command is logged.
- Summarize DATA stream
  A line count and byte count summary of the DATA stream is logged.
- Echo DATA stream
  The entire DATA stream is logged.

Note: For outbound messages, the DATA stream is buffered (the line count and byte count of the DATA stream for outbound messages will not match the line count and byte count for inbound messages).

Chapter 4

Setting your blocking policy

This chapter includes the following topics:

- About your blocking policy
- Blocking by message criteria
- Blocking by container file limits
- Blocking if an encrypted container is detected
- Blocking spam
- Preventing spam relaying

About your blocking policy

Your blocking policy is determined by how you configure Symantec AntiVirus for SMTP Gateways to block messages (what criteria to use to block messages and attachments, and how those blocked messages and attachments are to be handled).

Table 4-1 shows criteria that you can use to block messages and attachments, and how those blocked messages and attachments can be handled.

Table 4-1 Blocking criteria

Criteria	Handling options
Message size	Email messages that exceed the size that is specified in megabytes are not accepted at the SMTP server. Not blocking messages based on size is the default.
Subject line	Email messages with specified subject lines may be dropped, logged, or forwarded. Not identifying subject lines is the default.
File name	Email messages with specified file names may be delivered with their attachments dropped. Not deleting attachments based on file names is the default, though a suggested extension list is provided.
Container limit	Email messages that exceed any of the specified container limits may be dropped. Blocking messages that exceed container limits is the default.
Encrypted container	Email messages that are encrypted or password protected have their containers deleted and the messages delivered, the messages and containers dropped, the incidents logged and the messages with containers delivered, or the messages and containers forwarded to a specified address. Deleting the containers and delivering the messages is the default.
Sender’s address	Email messages that are from specified email addresses or domains are blocked. Not blocking messages based on sender’s address is the default.
DNSBL antispam list	Email messages that are from domains listed in the Domain Name Server black list (DNSBL) services you specify are blocked.
Anti-relay settings	Email messages with non-local destinations are handled according to how you configure Symantec AntiVirus for SMTP Gateways. Do not allow, except for listed hosts is the default.

Table 4-1 Blocking criteria

Criteria	Handling options
Characters in addresses	Email messages with characters specified to be blocked are not accepted at the SMTP server. Not blocking by characters in email addresses is the default.

Blocking by message criteria

Symantec AntiVirus for SMTP Gateways can be configured to block messages based on the following content:

- Message size
  See "Blocking by message size" on page 69.
- Subject line
  See "Blocking by subject line" on page 70.
- File name
  See "Blocking by file name" on page 70.

Blocking by message size

You can configure Symantec AntiVirus for SMTP Gateways to block email by message size.

To block by message size

1. On the Symantec AntiVirus for SMTP Gateways administrative interface, in the left pane, click **Blocking Policy.**
2. In the Content window, on the Configure tab, under Blocking by message size, check **Reject messages that are greater than** [ ] **megabytes.**
   Default is 50.
3. In the text box, type the number of megabytes that must be exceeded for a message to be rejected.
   Do not use a decimal.
4. Click **Save Changes.**

Blocking by subject line

You can configure Symantec AntiVirus to block email by subject line.

To block by subject line

1. On the Symantec AntiVirus for SMTP Gateways administrative interface, in the left pane, click **Blocking Policy**.
2. In the Content window, on the Configure tab, under Blocking by subject line, check **Identify the following subject lines (one per line) as content violations.**
3. In the subject line box, type subject lines, one per line, that Symantec AntiVirus for SMTP Gateways will block.

   Subject line blocking is not case sensitive.

   You can use the * and ? wildcards, for example, *hot* would block any subject line that contains the word hot.
4. Under Take the following action when a subject line violation occurs, select one of the following:
   - Drop message
   - Log only
   - Forward message
5. If you selected Forward message, in the To email address box, type one address to which the rejected message will be forwarded and in the Subject line box, type the subject line of the rejected message to be forwarded.
6. Click **Save Changes.**

Blocking by file name

You can configure Symantec AntiVirus for SMTP Gateways to block email by file name.

You can delete file names in the default list or add more file names to be blocked.

Table 4-2 shows the extensions that Symantec AntiVirus for SMTP Gateways blocks by default when you enable blocking by file name.

Table 4-2 Extension default blocking list

File extension	Description
*.ad	After dark screen saver file

Table 4-2 Extension default blocking list

File extension	Description
*.ade	Microsoft Access Project extension
*.adp	Microsoft Access Project
*.asp	Active Server Pages file
*.bas	Visual Basic® Class module
*.bat	Batch file
*.chm	Compiled HTML Help File
*.cmd	Windows NT command script
*.com	MS-DOS® application
*.cpl	Control Panel extension
*.crt	Security certificate
*.exe	Application
*.hlp	Windows Help file
*.hta	HTML application
*.inf	Setup information file
*.ins	Internet communication settings
*.isp	Internet communication settings
*.js	JScript® file
*.jse	JScript encoded script file
*.lnk	Shortcut
*.mdb	Microsoft Access application
*.mde	Microsoft Access MDE database
*.msc	Microsoft common console document
*.msi	Windows installer package
*.msp	Windows installer patch
*.mst	Visual test source file

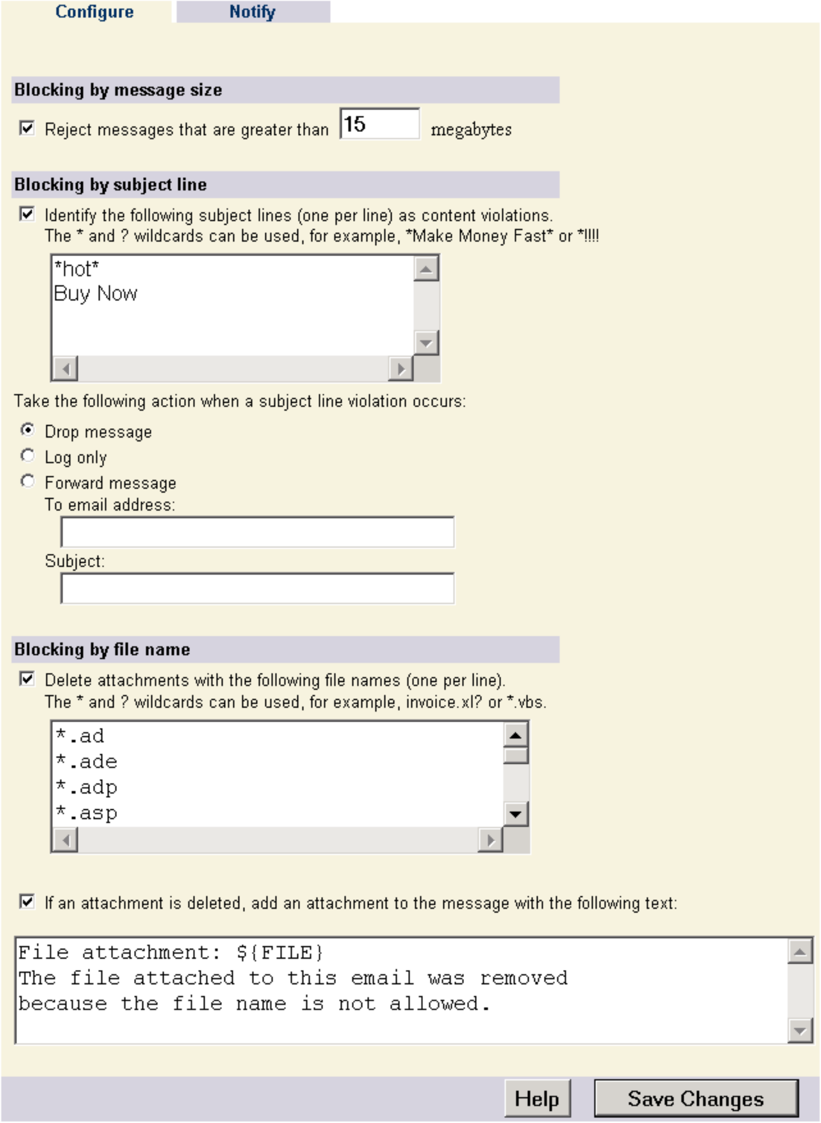
Table 4-2 Extension default blocking list

File extension	Description
*.pcd	Photo CD image
*.pif	Shortcut to MS-DOS program
*.reg	Registration entries
*.scr	Screen saver
*.sct	Windows script component
*.shb	Document shortcut file
*.shs	Shell scrap object
*.url	Internet shortcut (Uniform Resource Locator)
*.vb	VBScript file
*.vbe	VBScript encoded script file
*.vbs	VBScript script file
*.vsd	Visio® drawing file
*.vss	Visual SourceSafe file
*.vst	Targa bitmap file
*.vsw	Visio workspace file
*.ws	WordStar file
*.wsc	Windows script component
*.wsf	Windows script file
*.wsh	Windows scripting host settings file

Note: Entering only * or *.* will generate an error message.

To block attachments by file name

1 On the Symantec AntiVirus for SMTP Gateways administrative interface, in the left pane, click **Blocking Policy**.



Blocking by message size

☑ Reject messages that are greater than 15 megabytes

Blocking by subject line

☑ Identify the following subject lines (one per line) as content violations.
The * and ? wildcards can be used, for example, *Make Money Fast* or *!!!!

```
*hot*
Buy Now
```

Take the following action when a subject line violation occurs:

● Drop message
○ Log only
○ Forward message
To email address:

Subject:

Blocking by file name

☑ Delete attachments with the following file names (one per line).
The * and ? wildcards can be used, for example, invoice.xl? or *.vbs.

```
*.ad
*.ade
*.adp
*.asp
```

☑ If an attachment is deleted, add an attachment to the message with the following text:

```
File attachment: ${FILE}
The file attached to this email was removed
because the file name is not allowed.
```

2 In the Content window, on the Configure tab, under Blocking by file name, check **Delete attachments with the following file names (one per line)**.

Even though the blocking list is populated with default file names to be blocked, Symantec AntiVirus will not block attachments with those file names unless you check Delete attachments with the following file names.

3 Type one file name per line that you want blocked in the following format:

badnews.doc

You can use * for the file name or the extension.

4 To delete a default file name, highlight and delete the file name.

5 Check **If an attachment is deleted, add an attachment to the message with the following text.**

You can customize the message, if needed.

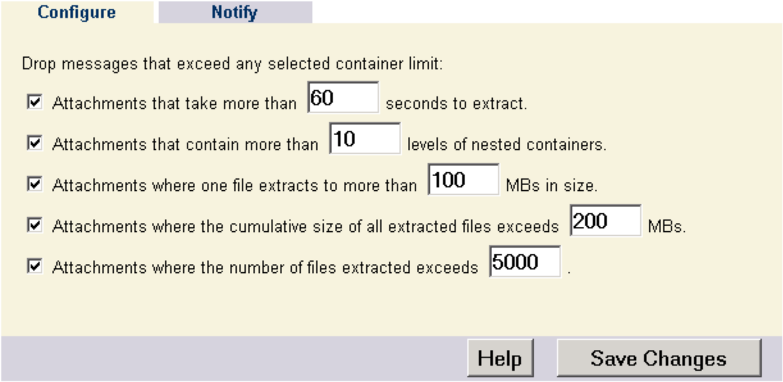
6 Click **Save Changes**.

Blocking by container file limits

You can configure Symantec AntiVirus for SMTP Gateways to protect against denial-of-service attacks that are associated with overly large container files that take a long time to decompose, and with files that contain multiple compressed files.

To block by exceeded container limit

1 On the Symantec AntiVirus for SMTP Gateways administrative interface, in the left pane, click **Blocking Policy**.



Drop messages that exceed any selected container limit:

☑ Attachments that take more than 60 seconds to extract.

☑ Attachments that contain more than 10 levels of nested containers.

☑ Attachments where one file extracts to more than 100 MBs in size.

☑ Attachments where the cumulative size of all extracted files exceeds 200 MBs.

☑ Attachments where the number of files extracted exceeds 5000 .

2 In the Container Limits window, on the Configure tab, check the container limit descriptors to be enabled when determining exceeded container limits.

3 Type the maximum allowable number for each enabled descriptor, or keep the defaults.

Do not type a zero (0) for the value.

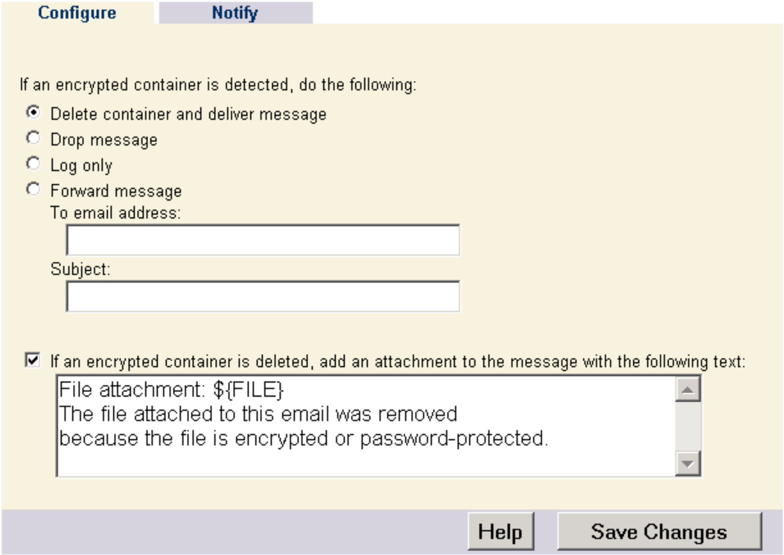
4 Click **Save Changes**.

Blocking if an encrypted container is detected

You can configure Symantec AntiVirus for SMTP Gateways to handle encrypted container files.

To block by encrypted container detection

1 On the Symantec AntiVirus for SMTP Gateways administrative interface, in the left pane, click **Blocking Policy**.



If an encrypted container is detected, do the following:

● Delete container and deliver message
○ Drop message
○ Log only
○ Forward message
To email address:
Subject:

☑ If an encrypted container is deleted, add an attachment to the message with the following text:

File attachment: ${FILE}
The file attached to this email was removed
because the file is encrypted or password-protected.

2 In the Encrypted Container window, on the Configure tab, select one of the following:

- Delete container and deliver message
- Drop message
- Log only
- Forward message

3 If you selected Forward message, in the To email address box, type the email address to which the message with the encrypted container should be forwarded and in the Subject box, type the subject that will appear in the subject line of the forwarded message.

4 To have a replacement attachment appended to the message from which an encrypted container has been deleted, check **If an encrypted container is deleted, add an attachment to the message with the following text**.

5 If you want to change the default text, in the text box, delete the default text and type the text that you want to appear in the replacement attachment.

6 Click **Save Changes**.

Blocking spam

Symantec AntiVirus for SMTP Gateways can block spam in the following ways:

- Block by a sender’s email address.
- Block by Domain Name Server black list (DNSBL) antispam lists.
  You can create an antispam white list so that email from the domains contained in the list are excluded from spam processing.
- Identify suspected spam messages by the heuristic spam engine.

Blocking by a sender’s email address

You can configure Symantec AntiVirus for SMTP Gateways to block email by a sender’s address or domain. It searches both the “envelope From” and “message From:” headers to determine string matches.

Domain names must begin with either @ or a period.

Note: If you configure Symantec AntiVirus for SMTP Gateways to block a subdomain (server.company.com, for example), it blocks only that subdomain and not the full domain (company.com, for example).

To block by a sender's address

1 On the Symantec AntiVirus for SMTP Gateways administrative interface, in the left pane, click **Blocking Policy**.

2 In the Anti-Spam window, on the Configure tab, under Blocking by sender's address, check **Identify messages from the following email addresses or domains as violations** (**one per line**).

3 In the text box, type the email addresses and domains to be blocked.
There must be only one entry per line.

4 Under Do the following when a violation occurs, select one of the following:

- Drop message
- Log only
- Forward message

5 If you selected Forward message, in the To email address box, type the email address to which the message will be forwarded and in the Subject box, type the subject that will appear in the subject line of the forwarded message.

6 Click **Save Changes**.

Blocking by DNSBL antispam lists

The most common way of preventing spam is rejecting mail that comes from mail servers known or believed to send spam. To limit potential spam, Symantec AntiVirus for SMTP Gateways can support up to three DNS black lists (DNSBL). DNSBL is a DNS-based blocking list generated to limit spam. You may choose to use these lists to reject or tag mail from certain sources, based on criteria determined by the list operators, such as return codes associated with Internet mail servers known to act as open relays or dial-up IPs used by spammers. DNSBL depends on an actively maintained DNS server with a database of IP addresses associated with Internet mail servers judged to be abusive on one or more spam-related criteria.

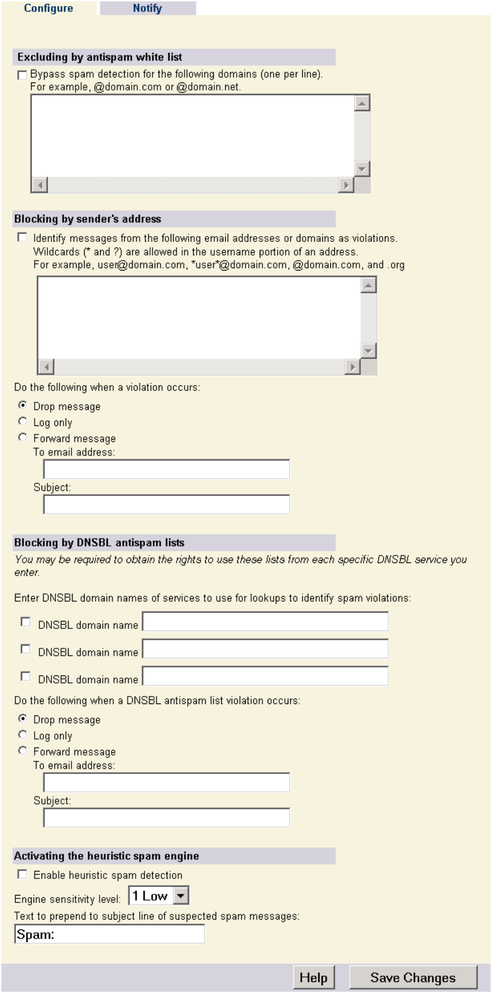
Symantec AntiVirus for SMTP Gateways uses the IP session of the open connection request from a sending mail host to query the DNSBL. If the query response indicates that the return code is listed in the DNSBL database, then Symantec AntiVirus for SMTP Gateways refuses the connection attempt.

In Symantec AntiVirus for SMTP Gateways, administrators can specify up to three domains to query against.

Note: If the check box for the DNSBL service is not checked, Symantec AntiVirus for SMTP Gateways does not attempt to use the service, even if a domain name is entered for a spam service.

To block by DNSBL antispam lists

1 On the Symantec AntiVirus for SMTP Gateways administrative interface, in the left pane, click **Blocking Policy**.



Excluding by antispam white list

□ Bypass spam detection for the following domains (one per line).
For example, @domain.com or @domain.net.

Blocking by sender's address

□ Identify messages from the following email addresses or domains as violations.
Wildcards (* and ?) are allowed in the username portion of an address.
For example, user@domain.com, *user*@domain.com, @domain.com, and .org

Do the following when a violation occurs:

● Drop message
○ Log only
○ Forward message
To email address:
Subject:

Blocking by DNSBL antispam lists

You may be required to obtain the rights to use these lists from each specific DNSBL service you enter.

Enter DNSBL domain names of services to use for lookups to identify spam violations:

□ DNSBL domain name
□ DNSBL domain name
□ DNSBL domain name

Do the following when a DNSBL antispam list violation occurs:

● Drop message
○ Log only
○ Forward message
To email address:
Subject:

Activating the heuristic spam engine

□ Enable heuristic spam detection

Engine sensitivity level: 1 Low

Text to prepend to subject line of suspected spam messages:
Spam:

2. In the Anti-Spam window, on the Configure tab, under Blocking by DNSBL antispam lists, check **DNSBL domain name**.
3. In the DNSBL domain name box, type the domain of the DNS service that you request.

   A check box will appear to let you identify spam by return codes. If desired, select the box, and a box will appear to let you type return codes to identify email as spam.
4. Type one return code per line (from the selected services) to identify email as spam.

   Identifying return codes means that only the email associated with the entered return codes will be blocked.

To handle antispam list violations

1. On the Symantec AntiVirus for SMTP Gateways administrative interface, in the left pane, click **Blocking Policy**.
2. In the Anti-Spam window, on the Configure tab, under Blocking by DNSBL antispam lists, under Do the following when a DNSBL antispam list violation occurs, select one of the following:
   - Drop message
   - Log only
   - Forward message
3. If you selected Forward message, in the To email address box, type one address to which the message will be forwarded and in the Subject line box, type the subject line to appear for the subject of the forwarded message.
4. Click **Save Changes**.

Excluding by antispam white list

You can choose to specify domains so that email from those domains is excluded from spam processing. If both DNSBL and exclusion are activated, Symantec AntiVirus for SMTP Gateways checks the antispam white list first when spam processing begins, after which the DNSBL black lists are queried. If the envelope sender matches a domain entered in the antispam white list, the email is allowed. If it does not match, DNSBL lists are checked. If there is a match, the email is blocked.

Email from domains listed in the white list are still processed for content violations and viruses.

To exclude by antispam white list

1. On the Symantec AntiVirus for SMTP Gateways administrative interface, in the left pane, click **Blocking Policy**.
2. In the Anti-Spam window, on the Configure tab, under Excluding by antispam white list, check **Bypass spam detection for the following domains** (**one per line**).
3. In the exclusion box, type domains (one per line) to be excluded from regular spam processing.

   Domain names must begin with either @ or a period.

   Note: You must have Bypass spam detection for the following domains (one per line) checked in order for the domains entered to bypass spam processing.

Identify suspected spam messages by the heuristic spam engine

You can choose to activate the heuristic spam engine in order to detect spam. The heuristic spam engine performs an analysis on the entire incoming email message, looking for key characteristics of spam. It weighs its findings against key characteristics of legitimate email, and assigns an accuracy rating (ex. 98%) to how certain it is that the message is spam. This rating, in conjunction with the engine sensitivity level (1=low, 5=high), determines whether a message is considered spam.

Note: One (1) is the default sensitivity level for the heuristic antispam engine. Increasing the sensitivity level may result in more false positives.

To identify suspected spam messages by the heuristic spam engine

1. On the Symantec AntiVirus for SMTP Gateways administrative interface, in the left pane, click **Blocking Policy**.
2. In the Anti-Spam window, on the Configure tab, under Activating the heuristic spam engine, do the following:
   - Select **Enable heuristic spam detection**.
   - Select the engine sensitivity level.
   - Type text that will appear in the subject line of suspected spam messages.
3. Click **Save Changes**.

Preventing spam relaying

Spam is unsolicited commercial email. You can configure relay restrictions within Symantec AntiVirus for SMTP Gateways so that it refuses to deliver email that has both a source and a destination outside of the organization (email for which neither the sender nor the receiver is local).

Another way that Symantec AntiVirus for SMTP Gateways prevents spam relaying is by rejecting messages with addresses that contain characters that are commonly associated with spam relaying, such as ! and %.

Configuring external relay restrictions

Two relay options are available:

- Allow: Relay restrictions are disabled for external hosts. Email from any remote host can be relayed through Symantec AntiVirus for SMTP Gateways to remote hosts.
- Do not allow, except for listed hosts (one per line): Relay restrictions are enabled for external hosts. Only email from explicitly named hosts and domains can be relayed to remote hosts.

  Do not allow, except for listed hosts (one per line) is the default.

The source of a message is the computer that contacts Symantec AntiVirus for SMTP Gateways, not the From address. The destination is the host portion of the recipient's address. If the source or destination is considered local, the Do not allow setting does not apply.

See "To configure external relay restrictions" on page 82.

If a message has multiple recipients, each recipient is considered individually for relay restrictions.

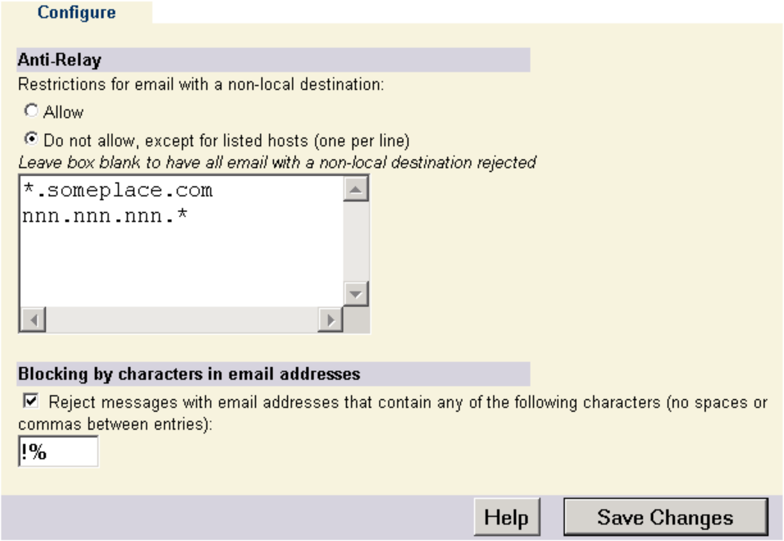
A source is considered local if Symantec AntiVirus for SMTP Gateways is running in Allow mode, or if the host is listed in the Do not allow, except for listed hosts list.

A destination is considered local if it is listed in the Local Routing list.

See "Configuring local routing" on page 55.

To configure external relay restrictions

1. On the Symantec AntiVirus for SMTP Gateways administrative interface, in the left pane, click **Blocking Policy**.



Configure

Anti-Relay

Restrictions for email with a non-local destination:

○ Allow

● Do not allow, except for listed hosts (one per line)

Leave box blank to have all email with a non-local destination rejected

```
*.someplace.com
nnn.nnn.nnn.*
```

Blocking by characters in email addresses

☑ Reject messages with email addresses that contain any of the following characters (no spaces or commas between entries):

!%

2. In the Anti-Relay window, on the Configure tab, select one of the following:
   - Allow
   - Do not allow, except for listed hosts (one per line)

3 If desired, type one host name, IP address, or domain per line for mail servers from which email will be allowed.

Domain name entries in this box will work only if the hosts have appropriate PTR records.

You can use the * wildcard to specify allowed hosts as the first element of a domain name or the last element of an IP address. For example:

*.someplace.com

1.2.3.*

1.2.*

1.*

If Do not allow is selected, and no hosts are listed, Symantec AntiVirus for SMTP Gateways rejects all email with a non-local destination.

4 Click **Save Changes**.

Blocking by characters in email addresses

You can configure Symantec AntiVirus for SMTP Gateways to reject messages with email addresses that contain characters that are commonly associated with spam relaying, such as ! and %.

To block by characters in email addresses

1 On the Symantec AntiVirus for SMTP Gateways administrative interface, in the left pane, click **Blocking Policy**.

2 In the Anti-Relay window, on the Configure tab, under Blocking by characters in email addresses, check **Reject messages with email addresses that contain any of the following characters**.

3 In the text box, type one or more characters for which Symantec AntiVirus for SMTP Gateways will search for email addresses to block.

Do not insert spaces or commas between the entries.

4 Click **Save Changes**.

Chapter 5

Setting your antivirus policy

This chapter includes the following topics:

- About your antivirus policy
- Configuring antivirus settings
- Configuring outbreak alerts
- Updating virus definitions files

About your antivirus policy

Your antivirus policy is determined by how you configure Symantec AntiVirus for SMTP Gateways to handle email (what file types to scan, what files to quarantine, and when to notify administrators and senders if viruses are found or virus outbreaks occur).

Configuring antivirus settings

You configure antivirus settings to have Symantec AntiVirus for SMTP Gateways do the following:

- Scan for viruses
  See "Enabling virus scanning" on page 86.
- Handle infected files
  See "Handling infected files" on page 88.
- Quarantine files
  See "Forwarding infected files to the Central Quarantine" on page 89.

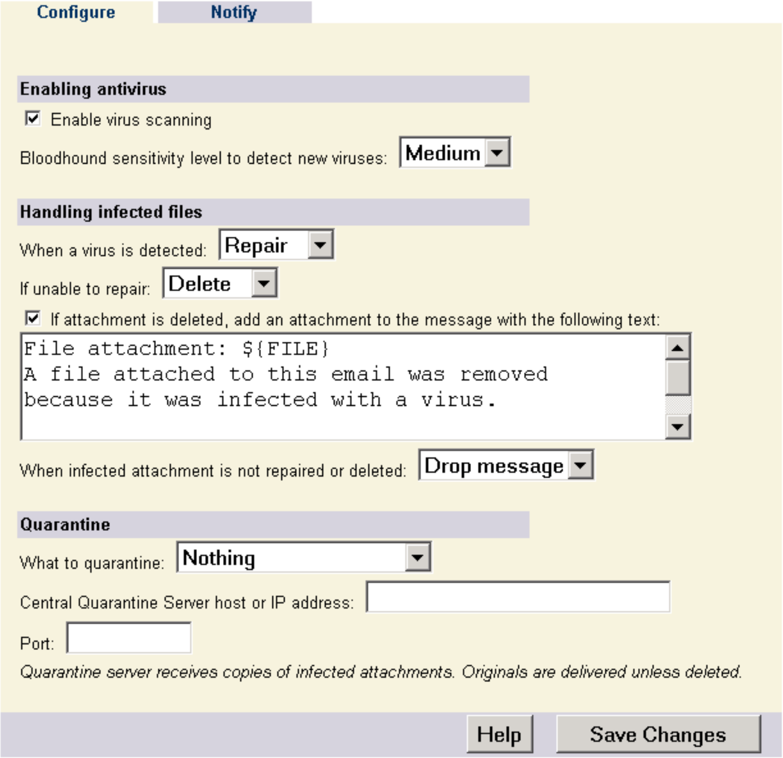
Enabling virus scanning

You must enable virus scanning and set the Bloodhound™ sensitivity level through the administrative interface. Bloodhound is the technology Symantec uses to heuristically detect new and unknown viruses.

Note: For information about the latest virus threats and other information about viruses, visit the Symantec Security Response Web site at www.sarc.com.

To enable virus scanning

1 On the Symantec AntiVirus for SMTP Gateways administrative interface, in the left pane, click **Antivirus Policy**.



Enabling antivirus

☑ Enable virus scanning

Bloodhound sensitivity level to detect new viruses: Medium

Handling infected files

When a virus is detected: Repair

If unable to repair: Delete

☑ If attachment is deleted, add an attachment to the message with the following text:

```
File attachment: ${FILE}
A file attached to this email was removed
because it was infected with a virus.
```

When infected attachment is not repaired or deleted: Drop message

Quarantine

What to quarantine: Nothing

Central Quarantine Server host or IP address:

Port:

Quarantine server receives copies of infected attachments. Originals are delivered unless deleted.

2 In the Antivirus window, on the Configure tab, under Enabling antivirus, ensure that Enable virus scanning is checked.

3 On the Bloodhound sensitivity level to detect new viruses drop-down list, select one of the following:

- Off
- Low
- Medium
- High

Medium is the default setting. If you set it to High, resource demand increases, performance may decrease, and occasional false positive detections may be generated.

4 Click **Save Changes**.

Note: Symantec AntiVirus for SMTP Gateways must be stopped and restarted for Bloodhound changes to take effect.

Handling infected files

Symantec AntiVirus for SMTP Gateways can handle infected files in a number of ways.

Scanning must be enabled and files must be specified for scanning in order for files to be processed.

See "Enabling virus scanning" on page 86.

To determine how infected files will be handled

1 On the Symantec AntiVirus for SMTP Gateways administrative interface, in the left pane, click **Antivirus Policy**.

2 In the Antivirus Settings window, on the Configure tab, under Handling infected files, on the When a virus is detected drop-down list, select one of the following:

- Repair: An attempt is made to repair the virus, and, if successful, the message is delivered.
- Delete: The infected file is deleted, and the message is delivered.
- Log only: Incident of the virus is logged, and the message (and the infected file) is delivered.

3 On the If unable to repair drop-down list, select one of the following:

- Delete: The infected file is deleted, and the message is delivered.
- Log only: Incident of the unrepairable virus is logged, and the message (with unrepairable file) is delivered.

4 If infected attachments are to be deleted, check **If attachment is deleted, add an attachment to the message with the following text** to add a notification message to the email.

You can retain the default message text, or modify it.

5. On the When infected attachment is not repaired or deleted drop-down list, select one of the following:
   - Drop message: Processing stops, and the message is dropped.
   - Log only: Incident of the infection is logged, and the message (and infected file) is delivered.
6. Click **Save Changes**.

Forwarding infected files to the Central Quarantine

Symantec AntiVirus for SMTP Gateways can forward infected attachments and files within attachments to a separately installed Central Quarantine server. The Central Quarantine must be installed on a Windows NT/2000 Server computer. Typically, heuristically detected viruses that cannot be repaired by the current set of virus definitions are forwarded to the Central Quarantine and isolated so that the viruses cannot spread.

From the Central Quarantine, these items are submitted to Symantec Security Response for analysis. If a new virus is identified, updated virus definitions are returned via LiveUpdate.

See "Updating virus definitions files" on page 91.

To establish quarantine settings

1. On the Symantec AntiVirus for SMTP Gateways administrative interface, in the left pane, click **Antivirus Policy**.
2. In the Antivirus Settings window, on the Configure tab, under Quarantine, on the What to quarantine menu, select one of the following:
   - Nothing
   - Unrepaired infections

     This setting functions only if Symantec AntiVirus for SMTP Gateways is configured to repair viruses.

     See "Handling infected files" on page 88.
   - All infections
3. In the Central Quarantine Server host or IP address box, type the host name or IP address of the server that is running the Central Quarantine.

4 In the Port box, type the port number for the Central Quarantine.

5 Click **Save Changes**.

Warning: If you configure Symantec AntiVirus for SMTP Gateways to forward infected files to the Central Quarantine, and the Central Quarantine is not running, files accumulate in the quarantine directory and may severely degrade performance.

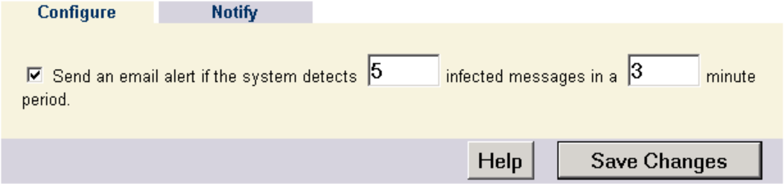
Configuring outbreak alerts

You can configure Symantec AntiVirus for SMTP Gateways to send notifications to one or more email addresses in cases of virus outbreaks.

Note: You must enter recipient addresses at Antivirus Policy > Outbreak Alert > Notify in order for this function to work.

To configure outbreak alerts

1 On the Symantec AntiVirus for SMTP Gateways administrative interface, in the left pane, click **Antivirus Policy**.



☑ Send an email alert if the system detects 5 infected messages in a 3 minute period.

2 In the Outbreak Alert window, on the Configure tab, check **Send an email alert if the system detects** [ ] **infected messages in a** [ ] **minute period**.

3 Type in the number of infected messages and the period of time in which those messages must be sent.

4 Click **Save Changes**.

Updating virus definitions files

Symantec AntiVirus for SMTP Gateways relies on up-to-date information to detect and eliminate viruses. Symantec supplies updated virus definitions files, which contain information about newly discovered viruses, to make sure that your protection is current. Updated files are provided at least once per week and whenever a new virus threat is discovered. When new virus definitions files are available, the LiveUpdate technology automatically downloads the proper files and installs them in the proper location. You can configure Symantec AntiVirus for SMTP Gateways to perform regular updates of virus definitions files via LiveUpdate, or you can set up your own LiveUpdate Server.

See “Setting up your own LiveUpdate server” on page 92.

Update virus definitions files

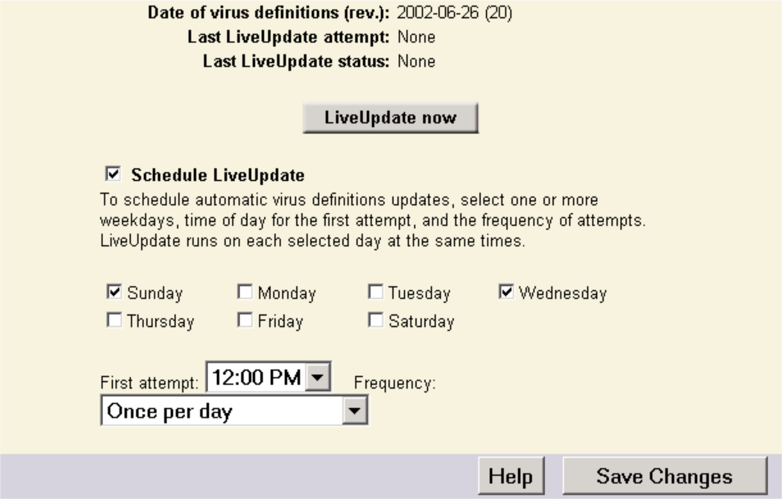
You can configure Symantec AntiVirus for SMTP Gateways to run LiveUpdate one or more days per week, the time of day for the first attempt, and the frequency of attempts. You can also update virus definitions manually at any time.

To schedule Automatic LiveUpdate

1. On the Symantec AntiVirus for SMTP Gateways administrative interface, in the left pane, click **LiveUpdate**.
2. In the LiveUpdate window, check **Schedule LiveUpdate**.
   Uncheck to disable a scheduled LiveUpdate.
3. Select one or more days on which you want LiveUpdate to run.
4. Select the time of the first attempt and the frequency of attempts.
   LiveUpdate runs on each selected day at the same time. For example, selecting Tuesday and Thursday, 06:00 AM, Once every four hours, causes LiveUpdate to run only on Tuesdays and Thursdays at 6:00 AM, 10:00 AM, 2:00 PM, 6:00 PM, and 10:00 PM. Since LiveUpdate considers midnight the end of the day, it would be invoked for the last time at 10:00 PM and would not be invoked again until 6:00 AM, which is designated as the first attempt.
5. Click **Save Changes**.

To update virus definitions manually

1 On the Symantec AntiVirus for SMTP Gateways administrative interface, in the left pane, click **LiveUpdate**.



Date of virus definitions (rev.): 2002-06-26 (20)
Last LiveUpdate attempt: None
Last LiveUpdate status: None

☑ Schedule LiveUpdate

To schedule automatic virus definitions updates, select one or more weekdays, time of day for the first attempt, and the frequency of attempts. LiveUpdate runs on each selected day at the same times.

☑ Sunday □ Monday □ Tuesday ☑ Wednesday
□ Thursday □ Friday □ Saturday

First attempt: 12:00 PM
Frequency: Once per day

2 In the LiveUpdate window, click **LiveUpdate now**.

Do not resubmit a LiveUpdate request. It may take a few minutes to contact a LiveUpdate server to determine if new updates are available.

Setting up your own LiveUpdate server

Using the LiveUpdate Administration Utility on the Symantec AntiVirus for SMTP Gateways CD, you can set up an intranet HTTP, FTP, or LAN server, or a directory on a standard file server to handle LiveUpdate operations for your network.

For more information, see the *LiveUpdate Administrator's Guide* on the Symantec AntiVirus for SMTP Gateways CD.

If you set up your own LiveUpdate server, you will need to edit the LiveUpdate configuration for Symantec AntiVirus for SMTP Gateways to point to the local LiveUpdate server. Contact Symantec Service and Support for more information.

Chapter 6

Notifications, logging, and reporting

This chapter includes the following topics:

- About the Status page
- About notifications
- Generating reports

About the Status page

When you log on to Symantec AntiVirus for SMTP Gateways, the Status page is displayed. This page shows system metrics that were calculated from the time of the most recent startup.

At the bottom of the window, you can click Refresh to update the display to reflect current, real-time status.

Note: Symantec AntiVirus for SMTP Gateways attempts a separate delivery for each recipient and the results are tracked individually. On the Status page, the number of Messages Delivered is often greater than the number of Messages Accepted because of multiple recipients.

Table 6-1 shows the information that appears on the Status page.

Table 6-1 Status page information

Topic	Information
System status	■ Server and port number for Symantec AntiVirus for SMTP Gateways ■ Version number of the product: 3.1.0.<version installed> ■ Date on which the server was last started ■ Amount of time that the server has been running since it was last started ■ Status of virus scanning: Enabled or Disabled ■ Status of Quarantine forwarding: All Files, Unrepairable Files, or Disabled ■ Total number of megabytes that have been received for processing since the server was last started ■ Message delivery status: Delivery or Pause ■ Incoming message status: Accept or Reject ■ Date of last virus definitions update (and latest revision number) ■ Date and time of last LiveUpdate attempt ■ Outcome of last LiveUpdate attempt: Succeeded or Failed ■ Date on which the SSL certificate was installed, or Not installed ■ Total number of repaired, deleted, and logged viruses

Table 6-1 Status page information

Topic	Information
Messages	■ Accepted: Number of messages added to the fast queue since the server was last started ■ Rejected: Number of messages rejected because the software is configured to reject messages, disallowed characters are in an email address, an anti-relay violation occurs, or the configured message size has been exceeded ■ Delivered: Number of outgoing messages that have been delivered ■ Dropped: Number of messages dropped because the software is configured to drop messages in any of the following cases: attachments are not repaired or deleted, subject lines are disallowed, container limit has been exceeded, encrypted container has been detected, disallowed sender's address has been detected, block by antispam list, scan error, scan failure ■ Held: Number of messages that have been added to the hold queue since last restart, including those dropped by the administrator. ■ Forwarded: Number of messages that have been forwarded successfully to the administrator addresses See "To set administrator email addresses for notifications and alerts" on page 42.
Infections	■ Repaired: Number of files that had viruses repaired ■ Deleted: Number of files that had viruses deleted ■ Logged: Number of files that had viruses logged only ■ Quarantined: Number of files that have been added to the Quarantine
Queue status	■ Number of messages currently in fast queue ■ Number of messages currently in slow queue ■ Number of messages currently in hold queue
Attachments	■ Number of top-level attachments that have been stripped from a message

About notifications

You can configure Symantec AntiVirus for SMTP Gateways to send notifications to senders and administrators when antivirus and blocking policies have been violated.

Understanding sender notifications

Table 6-2 shows sender notification information.

Table 6-2 Sender notification information

Event	Default subject	Default message	Other information
Virus found	Virus found in message you sent	A virus was found in a message sent by this account.	Virus information
Content violation	Content violation	Content violation found in email message.	■ From/To information ■ Content violation that occurred
Attachment too large	Attachment too large	A message sent by this account contains an attachment that is too large or expands into too much data.	From/To information
Encrypted attachment	Encrypted attachment	A message sent by this account contains encrypted or password-protected data.	From/To information
Spam **Note:** Notification is not sent when spam is detected by the heuristic spam engine.	Email not allowed	A message sent by this account comes from a domain or host not allowed by this mail server.	From/To information

Understanding administrator notifications

Administrator email addresses for all alerts other than virus outbreak are configured at Configuration > Accounts.

Table 6-3 shows administrator notification information.

Table 6-3 Administrator notification information

Event	Default subject	Default message	Other information
Virus found	Virus found	A virus was found in an email message.	■ From/To information ■ How message was handled (dropped) ■ Virus information

Table 6-3 Administrator notification information

Event	Default subject	Default message	Other information
Virus outbreak **Note:** Administrator email addresses for virus outbreak alert is configured at Antivirus Policy > Outbreak Alert > Notify.	Virus outbreak	Virus outbreak threshold has been exceeded. There is a possible virus outbreak.	None
Content violation	Content violation	Content violation found in email message.	■ From/To information ■ How message was handled (dropped, logged, or forwarded) ■ What content violation occurred
Exceeded container limit	Container violation	Container size violation found in email message.	■ From/To information ■ How message was handled (dropped, logged, or forwarded)
Encrypted container	Encrypted container	Encrypted container found in email message.	■ From/To information ■ How message was handled (dropped, logged, or forwarded)
Spam **Note:** Notification is not sent when spam is detected by the heuristic spam engine.	Spam violation	Spam violation found in email message.	■ From/To information ■ Spam information ■ How message was handled (dropped, logged, or forwarded)

Note: You can configure Symantec AntiVirus to send notification to multiple email addresses in the case of outbreak alerts.

Understanding notification metatags

Within the default text of notifications there are metatags, which act as placeholders for information. You can change text in any notification, but do not alter the metatags or you will not receive information about the event that triggered the notification.

Table 6-4 describes metatags and shows examples.

Table 6-4 Notification metatags

Metatag	Description	Example
MSGINFO	Tag in Content Violation notification to sender. Contains From/To information.	■ From: somebody@nnnn.com ■ To: someone@nnnn.com
DISPOSITION	Tag in Content Violation notification to administrator. Contains information about how the message was handled.	The message was dropped.
CONTENTINFO	Tag in Content Violation notification to administrator and sender. Contains content filter-specific data for the following: ■ Subject line blocked ■ Container limit exceeded ■ File name blocked	■ Subject: <specified by user> Matching Subject: <subject line matched> ■ The extracted attachment depth exceeded set limits. ■ File: <list of blocked file names> Matching file name: <file name matched>
VIRUSINFO	Tag in Virus Found notification to sender. Contains virus-specific data, such as virus name and signature number.	Virus scan results follow <list of specific virus information>
SPAMINFO	Tag in Spam Violation notification to administrator. Contains spam-specific data such as the rule that was used to block a particular message.	■ From: <from address> ■ Matching list: <matching list>
FILE	Tag in Filename Block notification to recipient. Contains the file name of the attachment that was deleted.	■ File(s): <list of blocked files> ■ Matching file names: <file names that triggered block>

Configuring notifications

You can configure Symantec AntiVirus for SMTP Gateways to send sender and administrator notifications when the following is detected:

- Infected file
- Outbreak alert
- Content violation
- Container limit violation
- Encrypted container
- Antispam list violation

Notifications are configured on the Notify tabs in the product.

Note: Notification is not sent when spam is detected by the heuristic spam engine.

To configure notifications

1. On the appropriate Notify tab, check **Notify sender**, **Notify administrator**, or both.
2. If you selected to notify sender, under Notification for sender, either accept the default Subject and Message text or delete the default text and type your own.
3. If you selected to notify administrator, under Notification for administrator, either accept the default Subject and Message text or delete the default text and type your own.
4. Click **Save Changes**.

Note: Do not alter the metatags ({$MSGINFO}, for example). Metatags act as placeholders for information that will be included in notifications.

Generating reports

Symantec AntiVirus for SMTP Gateways generates two types of reports:

- Summary: Shows totals for message, infection, and virus activity. When viruses are found, it includes links to more information about the viruses.
  See "Generating summary reports" on page 100.
- Detail: Shows detailed information about message, infection, and virus activity (to include dates of occurrences and client IP addresses, for example).
  See "Generating detail reports" on page 103.

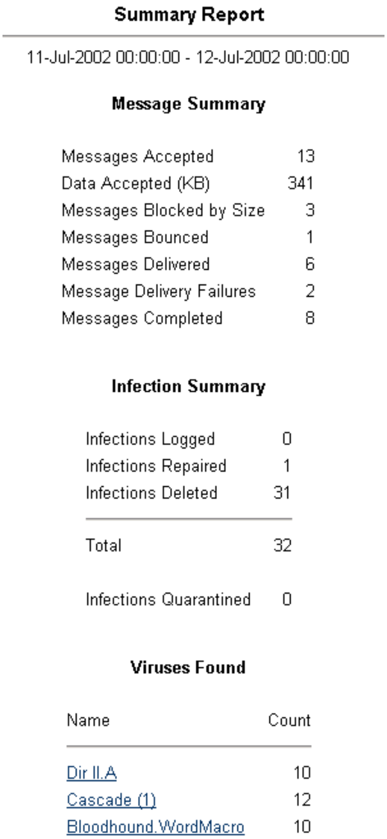
Generating summary reports

The summary report lists totals for virus infections and message processing, as well as the specific viruses detected.

To generate a summary report

1. On the Symantec AntiVirus for SMTP Gateways administrative interface, in the left pane, click **Reporting**.
2. On the Summary Report tab, on the From and To drop-down lists, select the date and time range for the report.

3 Click **Generate Report.**



Summary Report

11-Jul-2002 00:00:00 - 12-Jul-2002 00:00:00

Message Summary

Messages Accepted	13
Data Accepted (KB)	341
Messages Blocked by Size	3
Messages Bounced	1
Messages Delivered	6
Message Delivery Failures	2
Messages Completed	8

Infection Summary

Infections Logged	0
Infections Repaired	1
Infections Deleted	31
Total	32
Infections Quarantined	0

Viruses Found

Name	Count
Dir II.A	10
Cascade (1)	12
Bloodhound.WordMacro	10

- Message Summary: Shows totals for messages handled. See “About message summaries” on page 102.
- Infection Summary: Shows totals for infections handled. See “About infection summaries” on page 103.

When there is data logged for the following, there are three additional sections of the report that display:

- Viruses Found: Shows the virus name, the number of times that the virus was encountered during the designated time period, and a total for the number of viruses that were encountered. Selecting a virus name takes you to the Symantec Security Response Web site, where you can view specific data about the virus.
- Subjects Blocked: Appears only when emails have been rejected due to blocked subject lines. It shows the subject line that triggered the block during the designated time period, a total for each blocked subject line, and a grand total.
- Attachments Deleted: It shows the file names for attachments that were deleted during the designated time period, a total for each file name, and a grand total.

About message summaries

Table 6-5 includes message summary information.

Table 6-5 Message summary information

Action	Description
Messages accepted	Number of messages that were added to the fast queue
Data accepted (KB)	Cumulative size of messages
Messages rejected	Number of messages that were rejected because the software is configured to reject messages, disallowed characters are in an email address, an anti-relay violation occurs, the configured message size has been exceeded, mime headers contain non-standard SMTP line terminators, or messages contain NUL characters
Messages bounced	Number of incoming messages that were bounced
Messages delivered	Number of outgoing messages that were delivered
Message delivery failures	Number of outgoing messages that were returned due to delivery error
Messages completed	Number of messages that were processed by Symantec AntiVirus for SMTP Gateways
Encrypted files deleted	Number of encrypted files that were deleted

About infection summaries

Table 6-6 includes infection summary information.

Table 6-6 Infection summary information

Action	Description
Infections logged	Number of files logged
Infections repaired	Number of files that had viruses that were repaired
Infections deleted	Number of files that contained viruses that were deleted
Total infections	Number of viruses that were detected, repaired, deleted, and logged only
Infections quarantined	Number of files that are not deleted or repaired

Generating detail reports

A detail report contains all of the events in the Symantec AntiVirus for SMTP Gateways log. You can configure Symantec AntiVirus for SMTP Gateways to log entries for various lengths of time.

See "Configuring logging options" on page 61.

You can save the report in a comma-separated-value (CSV) format for import into spreadsheets or other graphical display software. The CSV report is saved in the log directory that was specified at installation (by default, \Program Files\Symantec\SAVSMTP\logs). The report file name is SAVSMTPyyyymmddhhmm.CSV, which indicates the date and time of creation.

Note: There are legacy fields (Mailbox and Mailbox ID) that are in the CSV report that are no longer used and are always empty.

To generate a detail report

1. On the Symantec AntiVirus for SMTP Gateways administrative interface, in the left pane, click **Reporting**.
2. On the Detail Report tab, on the From and To drop-down lists, specify the date and time range for the report.
3. Check the actions to include in the report.

4 In the Search box, you can type a single search term or string to narrow the output of the report.

The search is not case sensitive.

Note: If no actions are checked, the report contains all of the entries from the log.

5 Click **Generate Report** or **Write to CSV**.

The following are types of actions that can be included in a detail report:

- System: Associated with the operation of the Symantec AntiVirus for SMTP Gateways server

  See "About system actions" on page 104.
- SMTP: Associated with the transmission of mail between the server running Symantec AntiVirus for SMTP Gateways and other mail transfer agents (MTAs)

  See "About SMTP actions" on page 105.
- Message: Associated with email processing

  See "About message actions" on page 106.
- Blocking: Associated with blocking messages

  See "About blocking actions" on page 107.

About system actions

Table 6-7 shows the system actions.

Table 6-7 System actions

Action	Description
Logon	Shows the date and time of logon, the logon result (Succeeded/ Failed), the user who logged on, and the user's client IP address
Logoff	Shows the date and time of logoff, the logoff result (Succeeded/ Failed), the user who logged off, and the user's client IP address
LiveUpdate	Shows the date and time of the last LiveUpdate session and the LiveUpdate result (Succeeded/Failed)
Definitions updated	Shows the date and time of the last virus definitions update, the result of the update (Succeeded/Failed), and the date and revision number of the virus definitions update

Table 6-7 System actions

Action	Description
Object modified	Shows the date that information was changed through the administrative interface, what was modified, which user modified it and from which client, and the type of modification that was made
Service started	Shows the date and time that the Symantec AntiVirus for SMTP Gateways service started
Service start failed	Shows the date and time that the Symantec AntiVirus for SMTP Gateways service failed to start
Service stopped	Shows the date and time that the Symantec AntiVirus for SMTP Gateways service stopped
Reordering started	Shows the date and time that queue reordering started
Reordering stopped	Shows the date and time that queue reordering stopped, the number of messages moved to the front of the queue, and the number of seconds spent performing a queue reorder

About SMTP actions

Table 6-8 shows the SMTP actions.

Table 6-8 SMTP actions

Action	Description
Connection from	Shows the date and time that any mail client attempts to connect to the Symantec AntiVirus for SMTP Gateways server, the result of the connection (Succeeded/Failed), the client's IP address, and the connection ID
Connected to	Shows the date and time that Symantec AntiVirus for SMTP Gateways server attempts to connect to any mail server, result of the connection (Succeeded/Failed), connection ID, and connection information (Actual/Cached)
Disconnected	Shows which client or mail server was disconnected, the client ID, and the date and time of the disconnection
Connection closed	Shows the date and time that the connection was closed, IP address of the server connected to the Symantec AntiVirus for SMTP server, connection ID, last command sent, and last response sent by the disconnecting server

Table 6-8 SMTP actions

Action	Description
Protocol violation	Shows which client committed the violation, the connection ID, information about the protocol violation, and the date and time of the violation
Rejected	Shows that a message was rejected, which client it was rejected from, date and time of rejection, and reason for rejection

About message actions

Table 6-9 shows the message actions.

Table 6-9 Message actions

Action	Description
Accepted	Shows the date and time that a message was accepted, the From/To information, the subject, the client IP address, the connection ID, and the SMTP ID
Dropped	Shows the date and time that a message was dropped, From/To information, the reason for the drop, and the SMTP ID
Bounced	Shows the date and time that a message was bounced, To information, the reason for the bounce, and the SMTP ID
Delivered	Shows the date and time that a message was delivered, From/To information, the client IP address, the connection ID, and the SMTP ID
Delivery failed	Shows the date and time that a message was delivered and the SMTP ID
Completed	Shows the date and time that a message failed to be delivered, the client IP address, and the SMTP ID
Delivery suppressed	Shows the date and time that a message was not delivered, From/To information, and the SMTP ID

About blocking actions

Table 6-10 shows the blocking actions.

Table 6-10 Blocking actions

Action	Description
Virus logged	Shows the date that the virus was logged, From/To information, and the virus name
Files repaired	Shows the date that the file was repaired, From/To information, and the virus name
Files deleted	Shows the date that the file was deleted, From/To information, and the virus name
Files quarantined	Shows the date that the file was quarantined and the file name
Subjects blocked	Shows the date that the subject was blocked, From information, subject, and which word or phrase was matched in the subject
Scan error	Shows the date of the scan error, From/To information, and a description of the scan error
Sender blocked	Shows the date and time of the block and the sender address
Attachment deleted	Shows the matching file name, date and time that an attachment was deleted, From/To information, SMTP ID number, name of deleted file, and reason for file being deleted
Spam list block	Shows the date and time of the block, how the message was handled, From/To information, SMTP ID, and the reason for the block
Heuristic spam detection	Shows the date and time of the message detected by heuristic spam engine, IP address of client accepting the email from Symantec AntiVirus for SMTP Gateways, From/To information, subject, size of message (in bytes), SMTP ID, Info “Message is considered to be spam,” the spam definitions date, and the spam score (%)

Integrating Symantec AntiVirus for SMTP Gateways with SESA

This chapter includes the following topics:

- About SESA
- Configuring logging to SESA
- Interpreting Symantec AntiVirus for SMTP Gateways events in SESA
- Uninstalling the SESA Integration Package
- Uninstalling the local SESA Agent

About SESA

In addition to using standard local logging for Symantec AntiVirus for SMTP Gateways, you can also choose to log events to the Symantec Enterprise Security Architecture (SESA). SESA is an underlying software infrastructure and a common user interface framework. It integrates multiple Symantec Enterprise Security products and third-party products to provide a central point of control of security within an organization. It provides a common management framework for SESA-enabled security products, such as Symantec AntiVirus for SMTP Gateways, that protect your IT infrastructure from malicious code, intrusions, and blended threats.

SESA helps you increase your organization's security posture by simplifying the task of monitoring and managing the multitude of security-related events and products that exist in today's corporate environments. SESA includes an event management system that employs data collection services for events generated on computers that are managed by Symantec security products. The event categories and classes include antivirus, content filtering, network security, and systems management. The range of events varies depending on the Symantec applications that are installed and managed by SESA.

You can monitor and manage these security-related events through the SESA Console. The SESA Console is the common user interface that provides manageable integration of security technologies (Symantec or otherwise), Symantec Security Services, and Symantec Security Response. You can query, filter, and sort data to reduce the security-related events that you see through the SESA Console, which allows you to focus on threats that require your attention. You can configure alert notifications in response to events, and generate, save, and print tabular and graphical reports of event status, based on filtered views that you have created.

SESA is purchased and installed separately. SESA must be installed and working properly before you can configure Symantec AntiVirus for SMTP Gateways to log events to SESA.

For more information, see the SESA documentation.

Configuring logging to SESA

The logging of events to SESA is in addition to the standard local logging features for Symantec AntiVirus for SMTP Gateways. Logging to SESA is activated independently of standard local logging. If you have purchased SESA, you can choose to send a subset of the events logged by Symantec AntiVirus for SMTP Gateways to SESA.

See “Interpreting Symantec AntiVirus for SMTP Gateways events in SESA” on page 119.

To configure logging to SESA, you must complete the following steps:

- Configure SESA to recognize Symantec AntiVirus for SMTP Gateways. In order for SESA to receive events from Symantec AntiVirus for SMTP Gateways, you must run the SESA Integration Wizard that is specific to Symantec AntiVirus for SMTP Gateways on each computer that is running the SESA Manager. The SESA Integration Wizard installs the appropriate integration components for identifying the individual security product (in this case, Symantec AntiVirus for SMTP Gateways) to SESA.

  See “Configuring SESA to recognize Symantec AntiVirus for SMTP Gateways” on page 111.
- Install a local SESA Agent on the computer that is running Symantec AntiVirus for SMTP Gateways. The local SESA Agent handles the communication between Symantec AntiVirus for SMTP Gateways and SESA.

  See “Installing the local SESA Agent using the Agent Installer” on page 113.
- Configure Symantec AntiVirus for SMTP Gateways (through the administrative interface) to communicate with the local SESA Agent and to log events to SESA.

  See “Configuring Symantec AntiVirus for SMTP Gateways to log events to SESA” on page 118.

Configuring SESA to recognize Symantec AntiVirus for SMTP Gateways

To configure SESA to receive events from Symantec AntiVirus for SMTP Gateways, run the SESA Integration Wizard that is specific to Symantec AntiVirus for SMTP Gateways on each computer that is running the SESA Manager. The SESA Integration Wizard installs the appropriate integration components for identifying Symantec AntiVirus for SMTP Gateways to SESA. You must run the SESA Integration Wizard for each SESA Manager computer to which you are forwarding events from Symantec AntiVirus for SMTP Gateways.

Each product that interfaces with SESA has a unique set of integration components. The integration components for all products that interface with SESA are available when you purchase SESA and are not distributed with the individual security products. Thus, the SESA integration component is not part of the Symantec AntiVirus for SMTP Gateways software distribution package.

See “Uninstalling the SESA Integration Package” on page 120.

To configure SESA to recognize Symantec AntiVirus for SMTP Gateways

1. On the computer on which the SESA Manager is installed, insert the Symantec Event Manager CD into the CD-ROM drive.
2. At the command prompt, change directories on the CD to \SAV SMTP 3.1\Sesa.
3. At the command prompt, type:

   java -jar setup.jar

   The SESA Integration Wizard starts.
4. Click **Next** until you see the SESA Domain Administrator Information window.
5. In the SESA Domain Administrator Information window, type the specific information about the SESA Domain Administrator and the SESA Directory.

SESA Domain Administrator Name	The name of the SESA Directory Domain Administrator account.
SESA Domain Administrator Password	The password for the SESA Directory Domain Administrator account.
IP Address of SESA Directory	The IP address of the computer on which the SESA Directory is installed (may be the same as the SESA Manager IP address if both are installed on the same computer). If you are using authenticated SSL instead of SESA default, anonymous SSL, you must enter the host name of the SESA Directory computer. For example, mycomputer.com. For more information on SESA default, anonymous SSL and upgrading to authenticated SSL, see the *Symantec Enterprise Security Architecture Installation Guide*.
SSL Port	The number of the SESA Directory secure port. The default port number is 636.

6. Follow the on-screen instructions to install the appropriate SESA Integration Package and complete the SESA Integration Wizard.
7. Repeat steps 1 through 6 on each SESA Manager computer to which you are forwarding Symantec AntiVirus for SMTP Gateways events.

Installing the local SESA Agent using the Agent Installer

The local SESA Agent handles the communication between Symantec AntiVirus for SMTP Gateways and SESA and is installed on the same computer that is running Symantec AntiVirus for SMTP Gateways. The local SESA Agent is provided as part of the software distribution package for Symantec AntiVirus for SMTP Gateways. A separate installation package for installing the Agent, sesa_agent_installer, is located in the SESA_agent directory on the distribution CD for Symantec AntiVirus for SMTP Gateways.

If you have more than one SESA-enabled product installed on a single computer, these products can share a local SESA Agent. However, each product must register with the Agent. Thus, even if an Agent has already been installed on the computer for another SESA-enabled security product, you must run the installer to register Symantec AntiVirus for SMTP Gateways.

The local SESA Agent is preconfigured to listen on IP address 127.0.0.1 and port number 8086. Symantec AntiVirus for SMTP Gateways uses this information to communicate with the Agent. If you must change the IP address or port number for the Agent, you must do so through the SESA Console. (Once an Agent is installed, it is controlled through the SESA Console, even though it is running on the same computer that is running the security product.) You must also update, through the Symantec AntiVirus for SMTP Gateways administrative interface, the information that Symantec AntiVirus for SMTP Gateways uses to contact the local SESA Agent.

For more information, see the SESA documentation.

See “Configuring Symantec AntiVirus for SMTP Gateways to log events to SESA” on page 118.

Install the SESA Agent using The Symantec AntiVirus for SMTP Gateways SESA Agent Installer

To install the SESA Agent using the SESA Agent Installer that Symantec AntiVirus for SMTP Gateways provides, run the Installer on all computers on which Symantec AntiVirus for SMTP Gateways 3.1 is installed.

See “Uninstalling the local SESA Agent” on page 120.

To install the SESA Agent on Windows 2000 Server/Advanced Server

1. Log on to the computer on which you have installed Symantec AntiVirus for SMTP Gateways as administrator or with administrator rights.
2. Copy the executable (.exe) file to install the Agent from the Symantec AntiVirus for SMTP Gateways distribution CD onto the computer.

3. Run the .exe file.

4. Indicate that you agree with the terms of the Symantec license agreement, then click **Next**.

   If you indicate No, the installation is aborted.

5. From the list of products to register with SESA, select Symantec AntiVirus for SMTP Gateways.

   You can register only one product at a time. If you are installing the SESA Agent to work with more than one Symantec product, you must run the installer again for each product.

6. Under Choose Destination Location, select the location in which to install the local Agent, then click **Next**.

   The default location is C:\Program Files\Symantec\SESA.

   If the SESA Agent is already installed on the same computer, this option does not display.

7. In the Primary SESA Manager IP address or host name box, type the IP address or host name of the computer on which the primary SESA Manager is running.

   If SESA is configured to use anonymous SSL (the default setting), type the IP address of the primary SESA Manager. If SESA is configured to use authenticated SSL, type the host name of the primary SESA Manager (for example, computer.company.com).

8. In the Primary SESA Manager port number box, type the port number on which the SESA Manager listens.

   The default port number is 443.

9. If you are running a Secondary SESA Manager that is to receive events from Symantec AntiVirus for SMTP Gateways, do the following:

   - In the Secondary SESA Manager IP address or host name box, type the IP address or host name of the computer on which the Secondary SESA Manager is running.
   - In the Secondary SESA Manager port number box, type the port number on which the Secondary SESA Manager listens.

     The default port number is 443.

10 In the Organizational unit distinguished name box, type the organizational unit distinguished name to which the Agent will belong.

If the organizational unit is unknown or not yet configured, this setting can be left blank. Use the format shown in the example:

ou=Europe,ou=Locations,dc=SES,o=symc_ses

The domain(s) (dc=) portion of the path should correspond to the domain that is managed by the selected SESA Management Server.

11 Select one of the following:

- Start SESA Agent Automatically: The SESA Agent starts automatically whenever the computer is restarted.
- Start SESA Agent Manually: You must manually restart the SESA Agent each time that the computer is restarted.

12 Check **Check box here if you want the SESA Agent to start at installation completion** to have the SESA Agent start immediately after the installation finishes.

If you do not check the check box, you must manually start the SESA Agent after the installation is complete.

The installer proceeds from this point with the installation. When the installation is complete, the Agent is installed as a Windows 2000 service, and is listed as SESA AgentStart Service in the Services Control Panel.

To install the SESA Agent on Solaris

1 Log on as root to the computer on which you have installed Symantec AntiVirus for SMTP Gateways.

2 Do one of the following:

- Copy the shell (.sh) file to install the Agent from the Symantec AntiVirus for SMTP Gateways distribution CD onto the computer, and change directories to the location where you copied the file.
- Run the Agent Installer file from the Symantec AntiVirus for SMTP Gateways distribution CD.

3 Type **sh ./sesa_agent_installer.sh**, then press **Enter**.

4 Indicate that you agree with the terms of the Symantec license agreement, then press **Enter**.

If you indicate No, the installation is aborted.

5. From the list of products to register with SESA, select Symantec AntiVirus for SMTP Gateways.

   You can register only one product at a time. If you are installing the Agent to work with more than one Symantec product, you must run the installer again for each product.

6. Select the location in which to install the SESA Agent, then click **Next**.

   The default location is /opt/Symantec/SESA.

   If the SESA Agent is already installed on the same computer, this option does not display.

7. Do one of the following:

   - Type the IP address or host name of the computer on which the primary SESA Manager is running.

     If SESA is configured to use anonymous SSL (the default setting), type the IP address of the primary SESA Manager. If SESA is configured to use authenticated SSL, type the host name of the primary SESA Manager (for example, computer.company.com).
   - Type the port number on which the SESA Manager listens.

     The default port number is 443.

8. If you are running a Secondary SESA Manager that is to receive events from Symantec AntiVirus for SMTP Gateways, do the following:

   - Type the IP address or host name of the computer on which the Secondary SESA Manager is running.
   - Type the port number on which the Secondary SESA Manager listens.

     The default port number is 443.

9. Type the organizational unit distinguished name to which the Agent will belong.

   If the organizational unit is unknown or not yet configured, this setting can be left blank. Use the format shown in the example:

   ou=Europe,ou=Locations,dc=SES,o=symc_ses

   The domain(s) (dc=) portion of the path should correspond to the domain that is managed by the selected SESA Management Server.

10 Type one of the following to indicate whether the SESA Agent should start automatically on system boot:

- y: The SESA Agent starts automatically on system boot.
- n: You must manually restart the SESA Agent after each system boot.

11 Type one of the following to indicate whether the SESA Agent should start immediately after the installation finishes:

- y: The SESA Agent starts immediately after installation.
- n: You must manually start the SESA Agent after installation.

The installer proceeds from this point with the installation. Unless you indicated otherwise during the installation, the SESA Agent starts automatically when the installation is complete. You may need to stop and restart the SESA Agent. A transcript of the installation is save as /var/log/SESAAGENT-install.log for later review.

Installing the SESA Agent manually by command line

As an alternative to using the SESA Agent Installer, you can install the SESA Agent by command line.

Install the SESA Agent manually by command line

To install the SESA Agent, you do the following:

- Prepare to install the SESA Agent.
- Install the SESA Agent by command line.

To prepare to install the SESA Agent

1 On the computer on which Symantec AntiVirus for SMTP Gateways is installed, create a folder for the SESA Agent files.

For example, C:\Agent.

2 Insert the SESA CD1 - SESA Manager into the CD-ROM drive.

3 Copy the files from the \Agent folder on the CD and paste them in the newly created folder on the Symantec AntiVirus for SMTP Gateways computer.

4 In a text editor, open the **Agent.settings** file.

For example, C:\Agent\Agent.settings.

5 Change the value of the mserverip setting to the IP address of the SESA Manager to which Symantec AntiVirus for SMTP Gateways will forward events.

6 Save and close the **Agent.settings** file.

To install the SESA Agent by command line

1 On the computer on which Symantec AntiVirus for SMTP Gateways is installed, at the command prompt, change to the folder in which the SESA Agent files reside.

For example, C:\Agent.

2 At the command prompt, type the following:

java -jar agentinst.jar -a3015

3015 is a unique product ID to install the Agent for Symantec AntiVirus for SMTP Gateways. To remove the SESA Agent, you must use the same product ID parameter (for Symantec Web Security, 3015).

Optionally, you can append any of the following parameters:

-debug	Writes logging information to the screen
-log	Turns off the installation log and instructs the SESA Agent to write logging information to the Agntinst.log file in the local Temp directory

Configuring Symantec AntiVirus for SMTP Gateways to log events to SESA

After you have installed the local SESA Agent to handle communication between Symantec AntiVirus for SMTP Gateways and SESA, you must configure Symantec AntiVirus for SMTP Gateways to communicate with the Agent by specifying the IP address and port number on which the Agent listens. You must also ensure that logging to SESA has been activated. These settings are located on the Symantec AntiVirus for SMTP Gateways administrative interface.

To configure Symantec AntiVirus for SMTP Gateways to log events to SESA

1. On the Symantec AntiVirus for SMTP Gateways administrative interface, in the left pane, click **Configuration**.
2. On the Logging tab, under SESA logging, check **Enable SESA logging**.
3. In the SESA agent host box, type the IP address on which the local SESA Agent listens.

   The default setting is 127.0.0.1 (the loopback interface), which restricts connections to the same computer.
4. In the Port number box, type the TCP/IP port number on which the local SESA Agent listens.

   The port number you enter here must match the port number on which the local SESA Agent listens. The default port is 8086.
5. Click **Save Changes**.

Interpreting Symantec AntiVirus for SMTP Gateways events in SESA

SESA provides extensive event management capabilities, such as common logging of normalized event data for SESA-enabled security products like Symantec AntiVirus for SMTP Gateways. The event categories and classes include antivirus, content filtering, network security, and systems management. SESA also provides centralized reporting capabilities, including graphical reports. Currently, the events forwarded to SESA by Symantec AntiVirus for SMTP Gateways take advantage of the existing SESA infrastructure for events.

You can create alert notifications for certain events. Notifications include pagers, SNMP traps, email, and OS Event Logs. You can define the notification recipients, day and time ranges when specific recipients are notified, and custom data to accompany the notification messages.

For more information on interpreting events in SESA and on the event management capabilities of SESA, see the SESA documentation.

Uninstalling the SESA Integration Package

If Symantec AntiVirus for SMTP Gateways is no longer forwarding messages to SESA, you can uninstall the SESA Integration Package from each computer that is running the SESA Manager.

To uninstall the SESA Integration Package

1. On the taskbar, click **Start** > **Run**.
2. At the command prompt, type: **java -jar setup.jar -uninstall**

Uninstalling the local SESA Agent

The local SESA Agent is automatically uninstalled when you uninstall Symantec AntiVirus for SMTP Gateways. If more than one product is using the Agent, the uninstall script removes only the Symantec AntiVirus for SMTP Gateways registration and leaves the Agent in place. If no other security products are using the Agent, the uninstall script will uninstall the Agent as well.

Index

Symantec AntiVirus™ for SMTP Gateways

CD Replacement Form

CD REPLACEMENT: After your 60-Day Limited Warranty, if your CD becomes unusable, fill out and return 1) this form, 2) your damaged CD, and 3) your payment (see pricing below, add sales tax if applicable), to the address below to receive replacement CD. *DURING THE 60-DAY LIMITED WARRANTY PERIOD, THIS SERVICE IS FREE.* You must be a registered customer in order to receive CD replacements.

FOR CD REPLACEMENT

Please send me: ___ CD Replacement

Name ____

Company Name ____

Street Address (No P.O. Boxes, Please) ____

City ______________________________ State _______ Zip/Postal Code _______________

Country* ______________________________ Daytime Phone ______________________________

Software Purchase Date ____

*This offer limited to U.S., Canada, and Mexico. Outside North America, contact your local Symantec office or distributor.

Briefly describe the problem: ____

CD Replacement Price	$ 10.00
Sales Tax (See Table)	______
Shipping & Handling	$ 9.95
TOTAL DUE	______

SALES TAX TABLE: AZ (5%), CA (7.25%), CO (3%), CT (6%), DC (5.75%), FL (6%), GA (4%), IA (5%), IL (6.25%), IN (5%), KS (4.9%), LA (4%), MA (5%), MD (5%), ME (6%), MI (6%), MN (6.5%), MO (4.225%), NC (6%), NJ (6%), NY (4%), OH (5%), OK (4.5%), PA (6%), SC (5%), TN (6%), TX (6.25%), VA (4.5%), WA (6.5%), WI (5%). Please add local sales tax (as well as state sales tax) in AZ, CA, FL, GA, MO, NY, OH, OK, SC, TN, TX, WA, WI.

FORM OF PAYMENT ** (CHECK ONE):

___ Check (Payable to Symantec) Amount Enclosed $ _________ __ Visa __ Mastercard __ AMEX

Credit Card Number ____ Expires __________

Name on Card (please print) ______________________________ Signature ______________________________

**U.S. Dollars. Payment must be made in U.S. dollars drawn on a U.S. bank.

MAIL YOUR CD REPLACEMENT ORDER TO:

Symantec Corporation
Attention: Order Processing
555 International Way
Springfield, OR 97477 (800) 441-7234
Please allow 2-3 weeks for delivery within the U.S.